Assurance Activity Report for

Nokia 7x50 SR OS 20.10.R4 for 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-a4, and 7750 SR-a8 with maxp10-10/1Gb-msec-sfp+ and me12-10/1gb-sfp+ MDAs Security Target

Version 3.3

collaborative Protection Profile for Network Devices, Version 2.2e
and
Network Device collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption Version 1.2

AAR Version 1.4, 2021-10-19

Evaluated by:

2400 Research Blvd, Suite 395
Rockville, MD 20850

Prepared for:

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Nokia Corporation

The Author of the Security Target:
Acumen Security, LLC

The TOE Evaluation was Sponsored by:
Nokia Corporation

Evaluation Personnel:
Lead Evaluator: Dayanandini Pathmanathan
Tester: Dipdev Pudasaini
Evaluator: Brad Mitchell

Common Criteria Version
Common Criteria Version 3.1 Revision 5

Common Evaluation Methodology Version
CEM Version 3.1 Revision 5

Revision History

VERSION	DATE	CHANGES
0.1	2020-12-23	Initial Draft
0.2	2021-04-05	First Revision
1.0	2021-08-16	Second Revision, addressing updates to ST v3.1 and AGD v0.6
1.1	2021-08-19	Third Revision, addressing check out comments
1.2	2021-10-08	Fourth revision, addressing ECR comments
1.3	2021-10-18	Fifth revision, addressing ECR comments
1.4	2021-10-19	Sixth revision, addressing ECR comments

Contents

1 TOE Overview

The Nokia 7x50 SR OS 20.10.R4 for 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-a4, and 7750 SR-a8 with maxp10-10/1Gb-msec-sfp+ and me12-10/1gb-sfp+ MDAs (herein referred to as the TOE) is a network device with the high-performance, scale and flexibility supporting service providers, web scale and enterprise networks. The Nokia 7x50 routers utilize the Nokia's SR OS technology.

1.1 TOE Product Type

The TOE is a network device that is composed of hardware and software and offers a scalable solution to the end users. It satisfies all of the criterion to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e] and Network Device collaborative Protection Profile (NDcPP) Extended Package for MACsec Ethernet Encryption, Version 1.2 [MACsec v1.2].

2 Assurance Activities Identification

The Assurance Activities contained within this document include all those defined within the NDcPP 2.2e and PP_NDCPP_MACSEC_EP_V1.2 based upon the core SFRs and those implemented based on selections within the PPs/EPs.

3 Test Equivalency Justification

This analysis provides an explanation of the differences between each of the hardware models included within the Target of Evaluation (TOE) boundary and the impact each of the differences have on the TOE functionality.

The TOE is being tested against the collaborative Protection Profile for Network Devices (NDcPP v2.2e) and MACsec Ethernet Encryption Extended package (MACsec v1.2).

3.1 Architectural Description

The Target of Evaluation (TOE) is the Nokia 7x50 SR OS 20.10.R4. The supported chassis are:

- 7750 SR-7
- 7750 SR-12
- 7750 SR-12e
- 7750 SR-1e
- 7750 SR-2e
- 7750 SR-3e
- 7750 SR-a4
- 7750 SR-a8

3.1.1 TOE Description

The Nokia 7750 Service Routers (SR) portfolio delivers high-performance, scaling and flexibility to support a full array of IP services and functions for service provider, web scale and enterprise networks. The collection of 7750 SRs includes a wide range of physical platforms that share a mutual architecture and feature set. This allows Nokia customers to select the platform that best addresses their unique business goals and gratifies their scale, density, space, power, and value-added service requirements without compromising on quality or features. The 7750 Series are chassis-based routers. The Nokia 7750 Service Router supports a full array of network functions and services, achieving scale and efficiency without compromising versatility. It provides highly available service delivery mechanisms that maximize network stability and minimize service interruptions. Every Nokia 7750 series routing appliance is a whole routing system that provides a variety of high-speed interfaces (only Ethernet is within scope of the evaluation) for various scale of networks and various network applications. Nokia Networks service routers have common Nokia SR OS firmware, features, and technology for compatibility across all platforms.

Nokia SR OS firmware is mainly responsible for all functionalities and services provided by the routers. The routers can be access either via local console or via a network connection that is protected using the SSH protocol. Each time a user accesses the routers either via local console terminal connection or from the network remotely using SSH, the user must ensure to successfully authenticate itself with the correct credentials.

The Nokia routers also support MACsec functionality between compatible Nokia MACsec peer devices using the Media Dependent Adapter (MDA). The communication between these devices includes frames for ARP and Ethernet Control frames. In addition, it includes Destination MAC and Source MAC addresses in MACsec and MKA frames, which are not protected.

MACsec Key Agreement (MKA) protocol uses the Connectivity Association Key (CAK) to derive transient session keys called Secure Association Keys (SAKs). SAKs and other MKA parameters are required to sustain communication over the secure channel and to perform encryption and other MACsec security functions. SAKs, along with other essential control information, are distributed in MKA protocol control packets, also referred to

as MKPDUs. MACsec can be deployed in two modes:

- Point-to-point mode
- Point-to-multipoint mode

In the evaluated configuration, MACsec is configured individually on a point-to-multipoint Ethernet link including the bridge, so that a pair of MACsec devices connected by one device can be connected to the other device via bridge or directly. In order to establish the secured channel, the MACsec devices rely on a Connectivity Association Key (CAK) and utilize the MKA protocol to make and receive the successful secure connection.

To determine an authorized peer, both the devices must first exchange MKA frame, these devices must agree upon a shared key and MACsec cipher suite to set up a transmit Security Associations (SA). Once the connections are established, the MACsec frames will be transmitted between devices.

The Nokia devices support MDAs. The MDAs are pluggable adapter cards. They provide the physical interface connectivity to the devices. MDAs can be different in terms of connectivity and density configuration settings. Additionally, the MDA modules vary by chassis. Regardless, they provide the same functionality and security for the related chassis. MDA-XPs and MDAs support ethernet and multiservice interfaces. For this evaluation, the following is true:

- Routers 7750 SR-a4 and 7750 SR-a8 support 10-port 10/1GE MACsec MDA-a-XP
- Routers 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-7, 7750 SR-12 and 7750 SR-12e support MDA me12-10/1gb-sfp+.

3.1.2 OS, Processor, and Firmware Comparison

The following table compares the Operating System and CPU within each of the included TOE platforms:

TOE Model	Description of OS	Image version	Analysis
OS – This is the operating system running on the platform			
7750 SR-7	Nokia SR OS	20.10.R4	All models are running an identical version of Nokia SR OS image version 20.10.R4. There are no differences.
7750 SR-12	Nokia SR OS	20.10.R4	
7750 SR-12e	Nokia SR OS	20.10.R4	
7750 SR-1e	Nokia SR OS	20.10.R4	
7750 SR-2e	Nokia SR OS	20.10.R4	
7750 SR-3e	Nokia SR OS	20.10.R4	
7750 SR-a4	Nokia SR OS	20.10.R4	
7750 SR-a8	Nokia SR OS	20.10.R4	

TOE Model	Description of CPU	MACsec MDA	Analysis
CPU – This is the processor running on the platform			

TOE Model	Description of CPU	MACsec MDA	Analysis
7750 SR-7	Octeon II CN6645 (Cavium)	me 12 – 10/1gb-sfp+ Microarchitecture used: Microsemi VSC8258 Intellisec	All models are running the Cavium CN66xx platform with an Octeon 2 processor. The CPUs share the same Microsemi VSC8258 Intellisec microarchitecture, however they differ in MACsec MDA extension support. The Cavium CN6645 supports me12-10/1gb-sfp+ MDA with VSC8258 microarchitecture. The Cavium CN6635 supports 10-port 10/1GE with MACsec MDA-a-XP with VSC8258 microarchitecture. While the MDAs are different in physical support, they share same Microsemi VSC8258 Intellisec microarchitecture. The MDA can be operated on two modes, such as 10G and 1G. On both modes, the MDA provides the identical security for MACsec.
7750 SR-12	Octeon II CN6645 (Cavium)	me 12 – 10/1gb-sfp+ Microarchitecture used: Microsemi VSC8258 Intellisec	
7750 SR-12e	Octeon II CN6645 (Cavium)	me 12 – 10/1gb-sfp+ Microarchitecture used: Microsemi VSC8258 Intellisec	
7750 SR-1e	Octeon II CN6645 (Cavium)	me 12 – 10/1gb-sfp+ Microarchitecture used: Microsemi VSC8258 Intellisec	
7750 SR-2e	Octeon II CN6645 (Cavium)	me 12 – 10/1gb-sfp+ Microarchitecture used: Microsemi VSC8258 Intellisec	
7750 SR-3e	Octeon II CN6645 (Cavium)	me 12 – 10/1gb-sfp+ Microarchitecture used: Microsemi VSC8258 Intellisec	
7750 SR-a4	Octeon II CN6635 (Cavium)	10/1GE MACsec MDA-a-XP Microarchitecture used: Microsemi VSC8258 Intellisec	
7750 SR- a8	Octeon II CN6635 (Cavium)	10/1GE MACsec MDA-a-XP Microarchitecture used: Microsemi VSC8258 Intellisec	

3.1.3 Platform Differences

The following tables provide a description of the physical differences between hardware models. None of the listed hardware differences have any impact on the security functionality provided by the TOE. All operate identically.

Hardware Models	7750 SR-7	7750 SR-12	7750 SR-12e	7750 SR-1e	7750 SR-2e	7750 SR-3e	7750 SR-a4	7750 SR-a8
Rack Units	8RU	14RU	22RU	6RU	10RU	13RU	5RU	7RU
Through-put	400G FD (SFM6)	400G FD (SFM6)	1.2T FD (SFM6)	400G (HD)	800G (HD)	1.2T (HD)	200G (HD)	400G (HD)
Dimension	• Height (8 RU): 35.6 cm (14.02 in) • Width:	• Height (14 RU): 62.2 cm (24.49 in) • Width:	• Height (22 RU): 97.8 cm (38.5 in) • Width:	• Height (6 RU): 26.7 cm (10.5 in) • Width: 44.45 cm	• Height (10 RU): 44.5 cm (17.5 in) • Width:	• Height (13 RU): 57.8 cm (22.75 in) • Width:	• Height (5 RU): 22.23 cm (8.75 in) • Width: 48.26 cm	• Height (7 RU): 31.11 cm (12.25 in) • Width:

Hardware Models	7750 SR-7	7750 SR-12	7750 SR-12e	7750 SR-1e	7750 SR-2e	7750 SR-3e	7750 SR-a4	7750 SR-a8
	44.5 cm (17.5 in) • Depth (600 mm ETSIcompliant): 64.6 cm (25.51 in)	44.5 cm (17.5 in) • Depth (600 mm ETSIcompliant): 64.5 cm (25.39 in)	44.5 cm (17.5 in) • Depth (600 mm ETSIcompliant): 76.2 cm (30 in)	(17.5 in) • Depth (600 mm ETSIcompliant): 53.8 cm (21.2 in)	44.45 cm (17.5 in) • Depth (600 mm ETSIcompliant): 53.8 cm (21.2 in)	44.45 cm (17.5 in) • Depth (600 mm ETSIcompliant): 53.8 cm (21.2 in)	(19.0 in) • Depth (300 mm ETSI-compliant): 24.28 cm (9.56 in)	48.26 cm (19.0 in) • Depth (300 mm ETSI-compliant): 24.8 cm (9.56 in)
Power	SR-7 entire system = Worst case total power of 3750 W	SR-12 entire system = Worst case total power of 6480 W	SR-12e entire system = Worst case total power of 12000W	SR-1e entire system = Worst case total power of 1532W	SR-2e entire system = Worst case total power of 2762W	SR-3e entire system = Worst case total power of 3883W	SR-a4 entire system = Worst case total power of 711W	SR-a8 entire system = Worst case total power of 1297W
Operating Temp	From -41 to 104°F (5 to 40°C)	From 41 to 104°F (5 to 40°C)	From 41 to 104°F (5 to 40°C)	From -40 to 158°F (-40 to 70°C)	From -40 to 158°F (-40 to 70°C)	From -40 to 158°F (-40 to 70°C)	From -40 to 158°F (-40 to 70°C)	From -40 to 158°F (-40 to 70°C)
Memory	16GB	16GB	16GB	16GB	16GB	16GB	16GB	16GB
CPU	Octeon II CN6645 (Cavium)	Octeon II CN6645 (Cavium)	Octeon II CN6645 (Cavium)	Octeon II CN6645 (Cavium)	Octeon II CN6645 (Cavium)	Octeon II CN6645 (Cavium)	Octeon II CN6635 (Cavium)	Octeon II CN6635 (Cavium)

Table 3

3.2 Equivalency Analysis

The following sections provide a per category analysis of key areas of differentiation for each hardware model to determine the minimum subset to be used in testing. The areas examined will use the areas and analysis description provided in the supporting documentation for the NDcPP v2.2e.

The TOE is being evaluated against the collaborative Protection Profile for Network Devices (NDcPP v2.2e) and MACsec Ethernet Encryption Extended package (MACsec v1.2).

3.2.1 Platform/Hardware Dependencies

The TOE boundary is inclusive of all hardware required by the TOE. The hardware platforms do not provide any of the TSF. For the hardware appliances, the hardware within the TOE only differs by configuration and performance. The TOE does not have any hardware-specific dependencies. The two MACsec MDAs to be tested as part of the evaluation are the me12-10/1gb-sfp+, which is compatible with the 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-12e, 7750 SR-12, as well as the 7750 SR-7 series routers; and the 10-port 10/1GE MACsec MDA-a-XP that is

compatible with the 7750 SR-a4 and 7750 SR-a8 series routers. All the MACsec MDAs have the same Microsemi VSC8258 Intellisec microarchitecture. The ports work in 10G/1G SFP/SFP+ mode. 10G/1G is negotiated based on the SFP that is installed on the port.

The VSC8258 devices support 10G and 1G modes to operate and provide the entire functionality. The VSC8258 devices ensure full line-rate encryption on both 1 GbE and 10 GbE speeds over multimedia types.

10G and 1G provide identical functionality with reference to security. Both modes provide the same end-to-end MACsec functionality to provide the confidentially over the communication.

Result:

- There are no hardware dependencies.
- All appliances are equivalent.

3.2.2 Differences in TOE Software Binaries

The underlying OS is installed with the application-level software on each of the appliances. The primary OS for all models within the TOE is the Nokia SR OS 20.10.R4. There are no specific dependencies on the OS. Additionally, the primary OS that is installed as part of the product software is identical.

Result:

- There are no OS dependencies.
- All appliances are equivalent.

3.2.3 Differences in Libraries Used to Provide TOE Functionality

All libraries compiled in the TOE software are equal including the version of the library regardless of the platform for which the software is compiled. There are no differences between the included libraries.

Result:

• There are no differences in the included libraries.

3.2.4 TOE Management Interface Differences

The TOE is managed via either remote CLI session or Local CLI. These management options are available on all hardware platforms regardless of the configuration. There are no differences in the management interface for any platform.

Result:

• All Appliances are equivalent.

3.2.5 TOE Functional Differences

Each hardware model within the TOE boundary provides equal functionality. There are no differences in the way the user interacts with each of the devices or the services that are available for each of these devices on a per appliance series basis. For example, the user interaction with a 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-7, 7750 SR-12, or 7750 SR-12e is identical to that of an interaction with a 7750 SR-a4 or 7750 SR-a8. Each device within an appliance series runs the same version of software.

Result:

• There are no security functional differences between platforms in a series.

• All Appliances are equivalent.

3.3 Recommendations/Conclusion

Based on the analysis above, the following platforms will be tested:

Chassis	Processor	MACsec MDA	Testing Coverage
7750 SR-1e	Octeon II CN6645 (Cavium)	me12-10/1gb-sfp+	Full execution of NDcPP 2.2e testing and MACsec testing will be performed on 7750 SR-1e with me12-10/1gb-sfp+ MDA. 10/1gb are the only mode. MDA can be operated on any mode.
7750 SR-a4	Octeon II CN6635 (Cavium)	10-port 10/1GE MACsec MDA-a-XP	Full execution of NDcPP v2.2e and MACsec v1.2 will be performed on 7750 SR-a4 since the 10-port 10/1GE MACsec MDA-a-XP is only compatible with 7750 SR-a4 and 7750 SR-a8 devices.

The two MACsec MDA that would be tested as part of the evaluation are the me12-10/1gb-sfp+which is compatible with the 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-7, 7750 SR-12 and 7750 SR-12e series routers and the 10-port 10/1GE MACsec MDA-a-XP, which is compatible with the 7750 SR-a4 and 7750 SR-a8 series routers. The CAVP Cert #3969 covers the AES implementations for the Microsemi Intellisec 10G PHY me12-10/1gb-sfp+ MDA and 10-port 10/1GE MACsec MDA-a-XP. The software and the underlying hardware are the same for MACsec MDA.

4 Test Beds & Testing Conditions

4.1 Audit

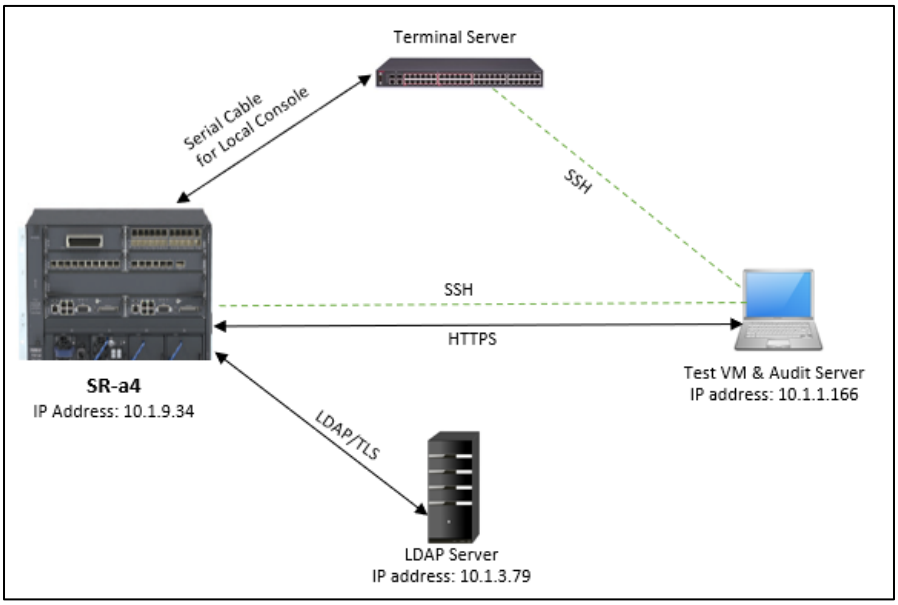

Figure 1. Device connection used in the testing.

Table 2. Details of each device used in testing.

Device Name	IP Address/Hostname	Relevance to Testing
SR-a4	10.1.9.34	TOE
Test VM (Ubuntu)	10.1.1.166	Test VM
Terminal Server	10.1.1.52	Terminal Server
VM (Ubuntu)	10.1.3.79	LDAP server, Audit server

4.2 Auth

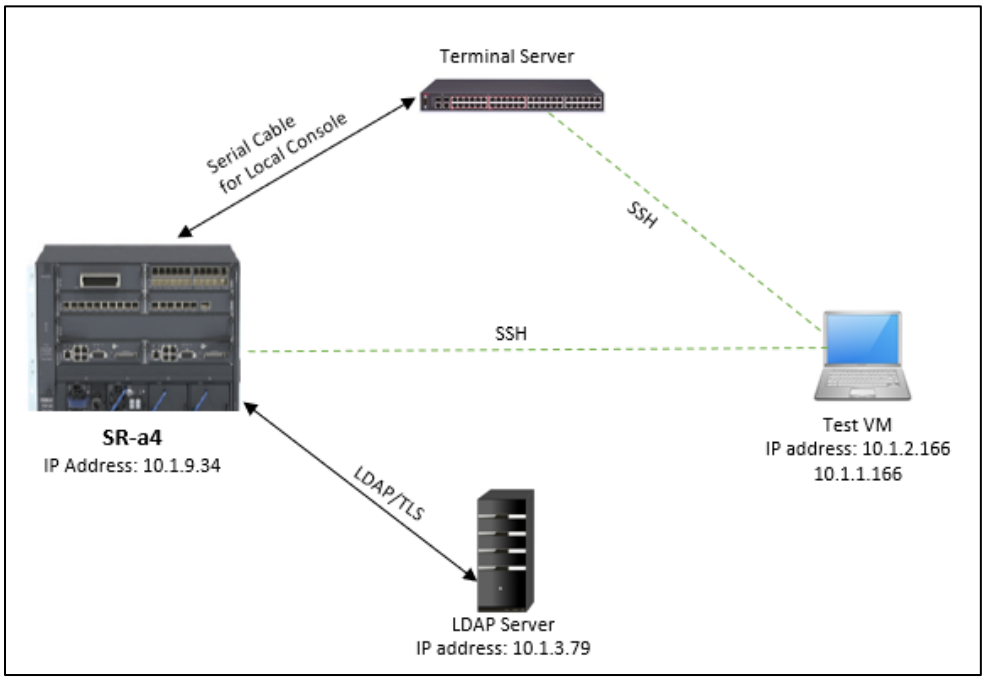

Figure 2. Device connection used in the testing.

Table 3. Details of each device used in testing.

Device Name	IP Address/Hostname	Relevance to Testing
SR-a4	10.1.9.34	TOE
Test VM (Kali)	10.1.2.166	Test VM
Test VM (Ubuntu)	10.1.1.166, 10.1.9.99	Test VM
Terminal Server	10.1.1.52	Terminal Server
System79	10.1.3.79	LDAP server

4.3 SSHS

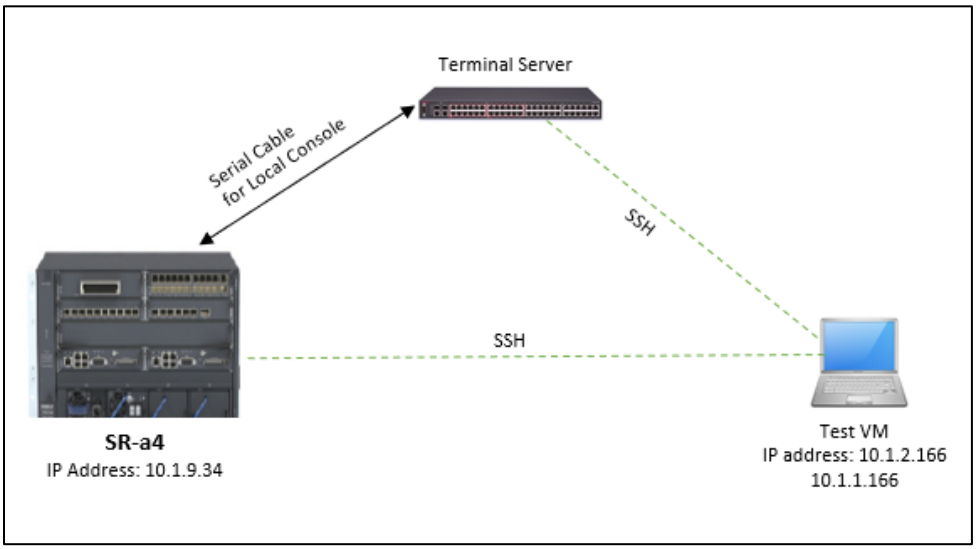

Figure 3. Device connection used in the testing.

Table 4. Details of each device used in testing.

Device Name	IP Address/Hostname	Relevance to Testing
SR-a4	10.1.9.34	TOE
Test VM (Kali)	10.1.2.166	Test VM
Test VM (Ubuntu)	10.1.1.166	Test VM
Terminal Server	10.1.1.52	Terminal Server

4.4 TLSC

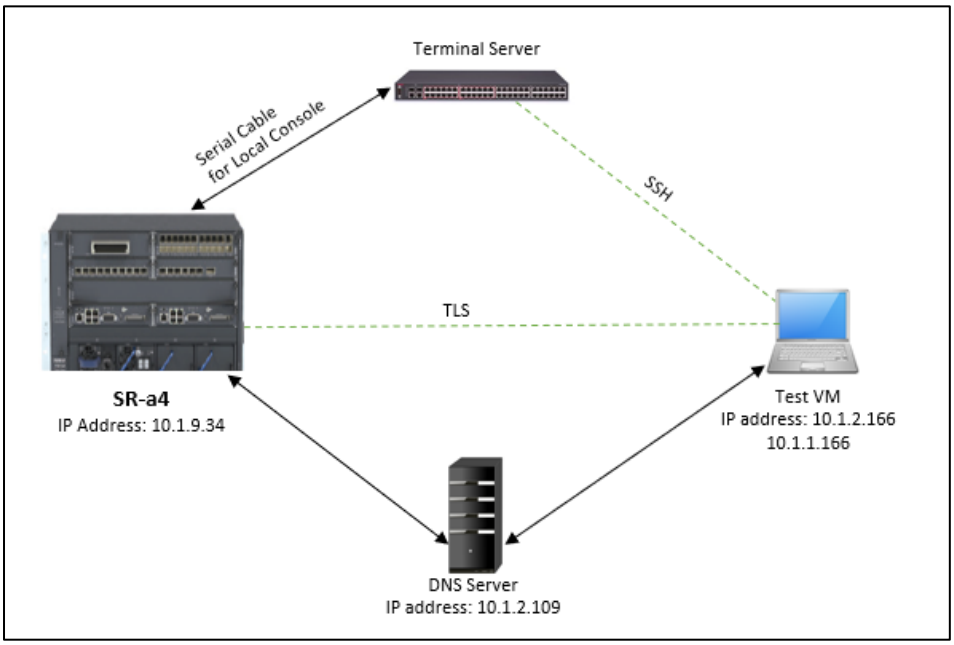

Figure 4. Device connection used in the testing.

Table 5. Details of each device used in testing.

Device Name	IP Address/Hostname	Relevance to Testing
SR-a4	10.1.9.34	TOE
Test VM (kali)	10.1.2.166	Test VM
Test VM (Ubuntu)	10.1.1.166	Test VM
DNS Server	10.1.2.109	DNS Server
Terminal Server	10.1.1.52	Terminal Server

4.5 Update

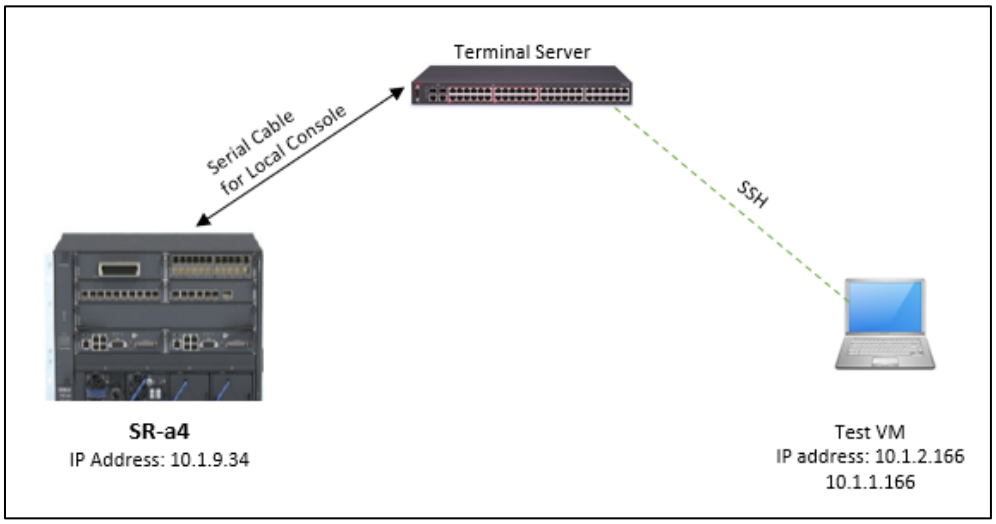

Figure 5. Device connection used in the testing.

Table 6. Details of each device used in testing.

Device Name	IP Address/Hostname	Relevance to Testing
SR-a4	10.1.9.34	TOE
Test VM (kali)	10.1.2.166	Test VM
Test VM (Ubuntu)	10.1.1.166	Test VM
Terminal Server	10.1.1.52	Terminal Server

4.6 X509-Rev

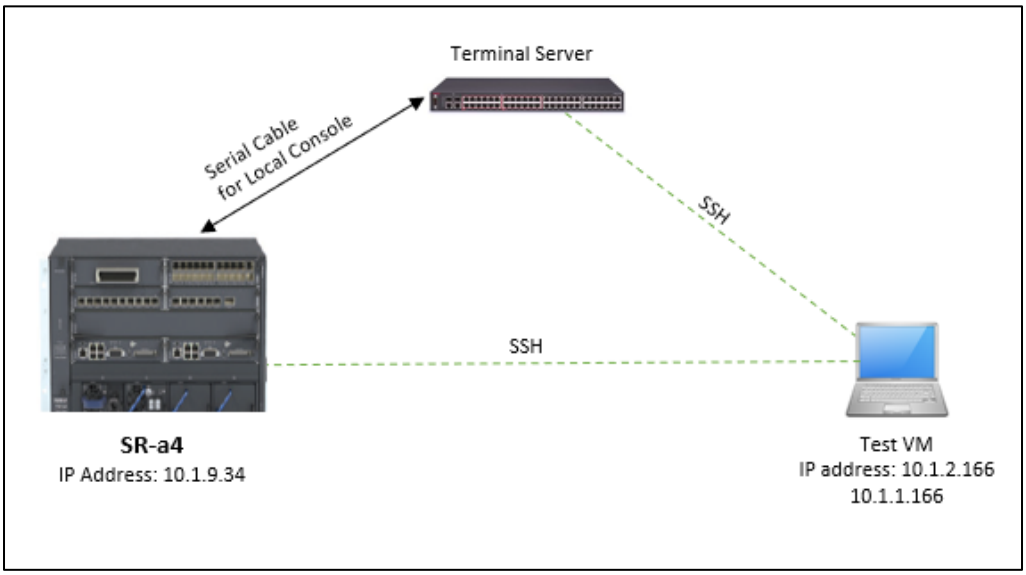

Figure 6. Device connection used in the testing.

Table 7. Details of each device used in testing.

Device Name	IP Address/Hostname	Relevance to Testing
SR-a4	10.1.9.34	TOE
Test VM (Kali)	10.1.2.166	Test VM
Test VM (Ubuntu)	10.1.1.166	Test VM
Terminal Server	10.1.1.52	Terminal Server

4.7 MACsec

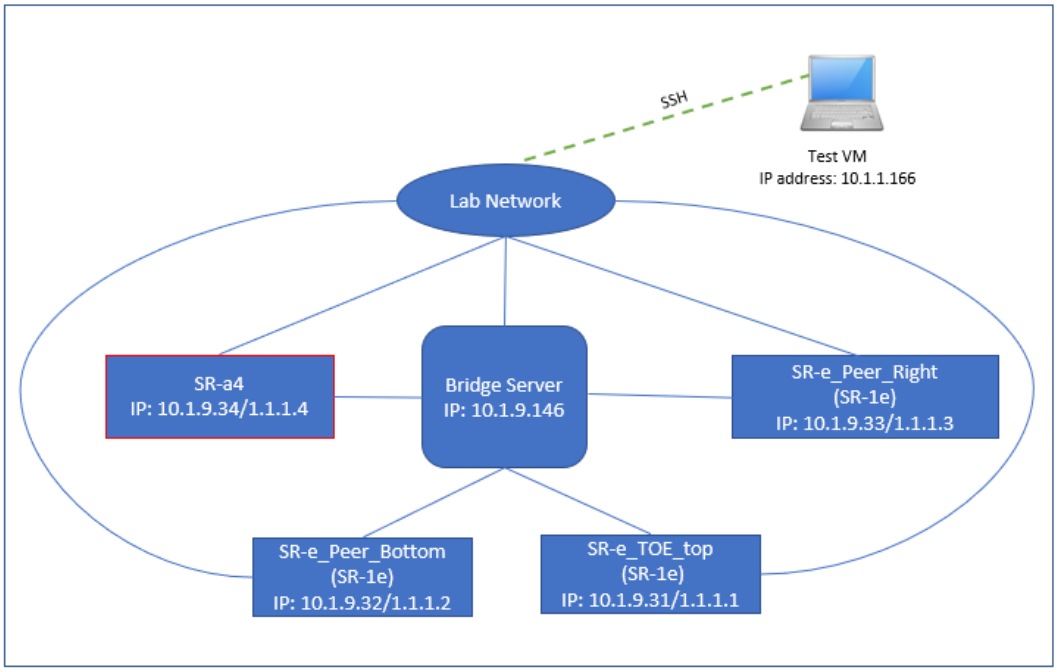

Figure 7. MACsec network diagram.

Table 8. Details of each device used in testing.

Device Name	IP Address/Hostname	Relevance to Testing
SR-a4	10.1.9.34/1.1.1.4	TOE
SR-e_TOE_top (SR-1e)	10.1.9.31/1.1.1.1	Peer A
SR-e_PeerB_bottom (SR-1e)	10.1.9.32/1.1.1.2	Peer B
SR-e_PeerC_Right (SR-1e)	10.1.9.33/1.1.1.3	Peer C
Bridge Server	10.1.9.146	Bridge
Test VM (Ubuntu)	10.1.1.166	Test VM

4.8 Test Time & Location

Some testing was carried out at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. The rest of the testing was performed locally using VPN access by the evaluator, Dipdev Pudasaini. Testing occurred from August 20, 2020 through July 23, 2021. Regression testing was performed on March 16th, 2021 and May 21st, 2021. The following tests were performed during regression testing to ensure ample coverage of all testing requirements:

FPT_TUD_EXT.1 Test #1

FIA_X509_EXT.1.1/Rev Test #2

FIA_X509_EXT.1.2/Rev Test #1

FCS_TLSC_EXT.1.1 Test #6b

FCS_SSHS_EXT.1.5 Test #3

FCS_SSHS_EXT.1.6 Test #2

FCS_MACSEC_EXT.2 Test #1

FTA_SSL.4 Test #1

FMT_MOF.1/Functions (1) Test #1

FIA_AFL.1 Test #2b

FPT_STM_EXT.1 Test #1

FPT_TST_EXT.1 Test #1

FAU_GEN.1

Testing was performed within Acumen's Common Criteria lab in a controlled, isolated environment and completed by the Acumen Security Evaluation Team following the CCTL's NVLAP-accredited test procedures.

4.9 Detailed Test Configuration

Test configuration for the SR-a4 as the TOE:

Name	OS	Version	Function	Protocols	IP address	MAC Address	Time	Tools (version)
SR-a4 (NOKIA 7750 SR-a4) (physical)	SROS	20.10.R4	TOE	SSH, TLS, MACsec, HTTPS, LDAP	10.1.9.34 1.1.1.4	20:e0:9c:9c:34:e9	Manually set and verified	
SR-e_TOE_top (physical)	SROS	20.10.R4	Peer A	SSH, MACsec	10.1.9.31 1.1.1.1	14:7b:ac:00:97:f9	Manually set and verified	
SR-e_Peer_Bottom (physical)	SROS	20.10.R4	Peer B	SSH, MACsec	10.1.9.32 1.1.1.2	a4:7b:2c:e1:16:15	Manually set and verified	
SR-e_Peer_Right (physical)	SROS	20.10.R4	Peer C	MACsec	10.1.9.33 1.1.1.3	a4:7b:2c:e1:16:21	Manually set and verified	
Bridge Server (physical)	Ubuntu	18.04	MACsec Bridge	MACsec, SSH	10.1.9.146	20:47:47:7e:92:80	Manually set and verified	Wireshark (2.6.10) Acumen

Name	OS	Version	Function	Protocols	IP address	MAC Address	Time	Tools (version)
								MACsec (1.2)
Lab Switch (physical)	IOS XE	15.2(5c)E	Lab switch		n/a	n/a	Manually set and verified	
Terminal Server			Serial connection to TOE		10.1.1.52		Manually set and verified	
Test VM (virtual)	Kali	2019.4	Test VM	SSH	10.1.2.166	00:0c:29:8e:50:36	Manually set and verified	OpenSSH (7.6) XCA (1.4.1) Acumen-tlsc Acumen-sshs Acumen-MACsec Wireshark (2.6.10)
Test VM (virtual)	Ubuntu	18.04	Test VM	SSH	10.1.1.166	00:0c:29:60:6c:07	Manually set and verified	OpenSSH (7.6) XCA (1.4.1) Acumen-tlsc Acumen-sshs Acumen-MACsec Wireshark (2.6.10)
Test VM (virtual)	Ubuntu	18.04	Test VM	SSH	10.1.9.99	00:0c:29:42:47:08	Manually set and verified	OpenSSH (7.6) XCA (1.4.1) Acumen-tlsc Acumen-sshs Acumen-MACsec Wireshark (2.6.10)
Authentication (LDAP) server (virtual)	Ubuntu	18.04	Authentication server	LDAP/TLS	10.1.3.79		Manually set and verified	2.4.45+dfsg-1ubuntu1.6 Nginx/ 1.14.0

Test configuration for the SR-1e as the TOE:

Name	OS	Version	Function	Protocols	IP address	MAC Address	Time	Tools (version)
SR-1e_TOE_top (NOKIA 7750 SR-1e)	SROS	20.10.R4	TOE	SSH, MACsec	10.1.9.31 1.1.1.1	14:7b:ac:00:97:f9	Manually set and verified	

(physical)								
SR-a4 (physical)	SROS	20.10.R4	Peer	SSH, TLS, MACsec, TLS, HTTP, LDAP	10.1.9.34 1.1.1.4	20:e0:9c:9c:34:e9	Manually set and verified	
SR-e_Peer_Bottom (physical)	SROS	20.10.R4	Peer B	SSH, MACsec	10.1.9.32 1.1.1.2	a4:7b:2c:e1:16:15	Manually set and verified	
SR-e_Peer_Right (physical)	SROS	20.10.R4	Peer C	MACsec	10.1.9.33 1.1.1.3	a4:7b:2c:e1:16:21	Manually set and verified	
Bridge Server (physical)	Ubuntu	18.04	MACsec Bridge	MACsec, SSH	10.1.9.146	20:47:47:7e:92:80	Manually set and verified	Wireshark (2.6.10) Acumen MACsec (1.2)
Lab Switch (physical)	IOS XE	15.2(5c)E	Lab switch		n/a	n/a	Manually set and verified	
Terminal Server			Serial connection to TOE		10.1.1.52		Manually set and verified	
Test VM (virtual)	Kali	2019.4	Test VM, Audit Server	SSH	10.1.1.205		Manually set and verified	OpenSSH (7.6) XCA (1.4.1) Acumen-tlsc Acumen-sshs Acumen-MACsec Wireshark (2.6.10)
Test VM (virtual)	Ubuntu	18.04	Test VM	SSH	10.1.1.166	00:0c:29:60:6c:07	Manually set and verified	OpenSSH (7.6) XCA (1.4.1) Acumen-tlsc Acumen-sshs Acumen-MACsec Wireshark (2.6.10)
Test VM (virtual)	Ubuntu	18.04	Test VM	SSH	10.1.9.99	00:0c:29:42:47:08	Manually set and verified	OpenSSH (7.6) XCA (1.4.1) Acumen-tlsc Acumen-sshs Acumen-MACsec Wireshark (2.6.10)
Authentication (LDAP) sever (virtual)	Ubuntu	18.04	Authentication server	LDAP/TLS	10.1.3.80		Manually set and verified	2.4.45+dfsg-1ubuntu1.6 Nginx/ 1.14.0

5 Detailed Test Cases (TSS and Guidance Activities)

5.1 TSS and Guidance Activities (Auditing)

5.1.1 FAU_GEN.1

5.1.1.1 FAU_GEN.1 TSS 1

Objective	For the administrative task of generating/import of, changing, or deleting of cryptographic keys as defined in FAU_GEN.1.1c, the TSS should identify what information is logged to identify the relevant key.
Evaluator Findings	The evaluator examined the [ST] Section 6 to determine the verdict of this assurance activity. The evaluator confirmed that within this section it identified the following information that was logged in order to identify the relevant key in relation to import/generation, changing, or deletion of cryptographic keys. Keys are identified by a unique string and a key size. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.2 FAU_GEN.1 Guidance 1

Objective	The evaluator shall check the guidance documentation and ensure that it provides an example of each auditable event required by FAU_GEN.1 (i.e. at least one instance of each auditable event, comprising the mandatory, optional and selection-based SFR sections as applicable, shall be provided from the actual audit record).
Evaluator Findings	The evaluator examined (AGD) section 4.4.2 to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the AGD provides an example of each type of audit log required by the PP and EP. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.1.3 FAU_GEN.1 Guidance 2

Objective	The evaluator shall also make a determination of the administrative actions related to TSF data related to configuration changes. The evaluator shall examine the guidance documentation and make a determination of which administrative commands, including subcommands, scripts, and configuration files, are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator shall document the methodology or approach taken while determining which actions in the administrative guide are related to TSF data related to configuration changes. The evaluator may perform this activity as part of the activities associated with ensuring that the corresponding guidance documentation satisfies the requirements related to it.
Evaluator Findings	The evaluator examined the AGD to verify that it identifies administrative commands, including subcommands, scripts, and configuration files, that are related to the configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the cPP. The evaluator examined the entirety of AGD to determine what administrative commands are associated with each

administrative activity. Upon investigation, the evaluator found that the following are applicable:

Administrative Activity	Section
administer the TOE locally	[AGD] section 2
Administer the TOE remotely	[AGD] section 2
Configure the access banner	[AGD] section 11.1
Configure the session inactivity timer	[AGD] section 10
Update the TOE	[AGD] section 8
Configure authentication failure parameters	[AGD] section 6.6
Generate a PSK-based CAK and install it in the TOE	[AGD] Section 5.3.2 Step 2
Manage the key server to create, delete, and activate MKA participants	[AGD] section 5.3.2 Step 12-16
Specify a lifetime of a CAK	[AGD] section 5.3.3
Enable, Disable, or Delete a PSK-based CAK	[AGD] section 5.3.2 describes enabling a PSK-based CAK. Disable: See "Delete" Delete: [AGD] section 5.3.2 step 4
Configure audit behavior	[AGD] section 4, 4.3, 4.4
Configure cryptographic functionality	[AGD] sections 5.3, 6.3.1, 6.5, and 7
Configure thresholds for SSH rekeying	[AGD] section 3.4.1
Set the time which is used for time-stamps	[AGD] section 9

Cause the key server to generate a new group CAK (aka,rekey the ca)[AGD] section 5.3.1 step 16

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2 FAU_STG_EXT.1

5.1.2.1 FAU_STG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes the means by which the audit data are transferred to the external audit server, and how the trusted channel is provided. Upon investigation, the evaluator found that the TSS states that a script is executed on the TOE to periodically transfer the log files from local storage to the secure server over HTTPS. [ST] section 6 states that the TOE uses HTTPS over TLS v1.2 to protect communications with the audit server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.2 FAU_STG_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes the amount of audit data that are stored locally; what happens when the local audit data store is full; and how these records are protected against unauthorized access. Upon investigation, the evaluator found that the TSS states that the TOE stores at most 6.8 GB of audit data on the local compact flash drive. If audit data storage is full, the TOE will overwrite the oldest log file. [ST] section 6 states “Only Authorized Administrators can access the audit events and have the ability to clear the audit events. The TOE does not allow non-privileged administrators to modify the audit records that are stored locally on the device.” Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.3 FAU_STG_EXT.1 TSS 3

Objective	The evaluator shall examine the TSS to ensure it describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs it contains a list of TOE components that store audit data locally. The evaluator shall examine the TSS to ensure that for distributed TOEs that contain components which do not store audit data locally but transmit their generated audit data to other components it contains a mapping between the transmitting and storing TOE components.

Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes whether the TOE is a standalone TOE that stores audit data locally or a distributed TOE that stores audit data locally on each TOE component or a distributed TOE that contains TOE components that cannot store audit data locally on themselves but need to transfer audit data to other TOE components that can store audit data locally. Upon investigation, the evaluator found that the TSS states that the TOE is a standalone entity. The evaluator examined the [ST] Section 6 to verify that, for distributed TOEs, the TSS contains a list of TOE components that store audit data locally. Upon investigation, the evaluator found that the [ST] does not describe a distributed or composed TOE. The evaluator examined the [ST] Section 6 to verify that, for distributed TOEs that contain components which do not store audit data locally, the TSS contains a mapping between the transmitting and storing TOE components. Upon investigation, the evaluator found that the [ST] does not describe or define a distributed or composed TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.4 FAU_STG_EXT.1 TSS 4

Objective	The evaluator shall examine the TSS to ensure that it details the behaviour of the TOE when the storage space for audit data is full. When the option 'overwrite previous audit record' is selected this description should include an outline of the rule for overwriting audit data. If 'other actions' are chosen such as sending the new audit data to an external IT entity, then the related behaviour of the TOE shall also be detailed in the TSS.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS details the behavior of the TOE when the storage space for audit data is full. Upon investigation, the evaluator found that the TSS states that the TOE overwrites the oldest log file and creates a new one. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.5 FAU_STG_EXT.1 TSS 5

Objective	The evaluator shall examine the TSS to ensure that it details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. In case the TOE does not perform transmission in realtime the evaluator needs to verify that the TSS provides details about what event stimulates the transmission to be made as well as the possible acceptable frequency for the transfer of audit data.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS details whether the transmission of audit information to an external IT entity can be done in realtime or periodically. Upon investigation, the evaluator found that the TSS states that audit data are transferred to the audit server at a configurable periodic interval, by configuring a CRON script on the TOE to execute in any configurable interval between 15 minutes to 1 week. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.6 FAU_STG_EXT.1 Guidance 1

Objective	The evaluator shall also examine the guidance documentation to ensure it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server.
Evaluator Findings	The evaluator examined (AGD) section 4.3 to verify that it describes how to establish the trusted channel to the audit server, as well as describe any requirements on the audit server (particular audit server protocol, version of the protocol required, etc.), as well as configuration of the TOE needed to communicate with the audit server. Upon investigation, the evaluator found that the AGD describes how to configure the TOE to send logs to the audit server over TLS. [AGD] section 4.1 and 4.2 describe the required configuration of the audit server as an rsyslog server, communicating over TLS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.7 FAU_STG_EXT.1 Guidance 2

Objective	The evaluator shall also examine the guidance documentation to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.
Evaluator Findings	The evaluator examined (AGD) section 4 to verify that it describes the relationship between the local audit data and the audit data that are sent to the audit log server. Upon investigation, the evaluator found that the AGD states that the TOE will store up to 6.8 GB of audit data. When storage space is full, the TOE will overwrite the oldest log file. Further, [AGD] instructs the administrator to configure the TOE to periodically transfer the locally-stored audit data to an external audit server, including how frequently the audit data are transferred. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.1.2.8 FAU_STG_EXT.1 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. The description of possible configuration options and resulting behavior shall correspond to those described in the TSS.
Evaluator Findings	[ST] section 5.2.1.3 selects only one option for FAU_STG_EXT.1.3, which is to overwrite the oldest log file. Because this behavior is not configurable, [AGD] does not describe the possible configuration options. This AA is not applicable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2 TSS and Guidance Activities (Cryptographic Support)

Note that Test activities in the SD that are typically addressed by referencing CAVP certs are addressed in this section and are identified as "Test/CAVP" activities.

5.2.1 FCS_CKM.1

5.2.1.1 FCS_CKM.1 TSS 1

Objective	The evaluator shall ensure that the TSS identifies the key sizes supported by the TOE. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS describes the TOE's key sizes as 2048-bit RSA keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.2 FCS_CKM.1 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target.
Evaluator Findings	The evaluator examined (AGD) section 3.1 to verify that it instructs the administrator how to configure the TOE to use the selected key generation scheme(s) and key size(s) for all cryptographic protocols defined in the Security Target. Upon investigation, the evaluator found that the AGD section 3 states that the TOE must be operated in FIPS-140-2 mode, and provide instructions on how to do so. [AGD] states that this will restrict the TOE to operating only in the approved modes. [AGD] section 7 describes how to configure the SSH and TLS protocols, which will only perform cryptographic functions in accordance with the FIPS-140-2 restricted mode. [AGD] section 6.5 describes how to generate a TLS keypair as part of a certificate signing request. [AGD] section 6.3 describes how to create a new SSH public key. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.1.3 FCS_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key generation mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: C2075, C2084 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2 FCS_CKM.2

5.2.2.1 FCS_CKM.2 TSS 1 [TD0580]

Objective	The evaluator shall ensure that the supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. If the ST specifies more than one scheme, the evaluator shall examine the TSS to verify that it identifies the usage for each scheme. It is sufficient to provide the scheme, SFR, and service in the TSS.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS supported key establishment schemes correspond to the key generation schemes identified in FCS_CKM.1.1. Upon investigation, the evaluator found that the TSS describes the supported key establishment as RSA according to PKCS1-v1_5 in RFC3447 Section 7.2 and FFC safe-primes according to RFC3526. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.2 FCS_CKM.2 Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected key establishment scheme(s).
Evaluator Findings	The evaluator examined (AGD) section 7 to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that putting the TOE in CC-NDcPP compliance mode restricts the TOE to only approved key establishment schemes. [AGD] section 3.1 describes how to enable the CC-NDcPP Compliance mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.2.3 FCS_CKM.1 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: C2075 and C2084 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3 FCS_CKM.4

5.2.3.1 FCS_CKM.4 TSS 1

Objective	The evaluator examines the TSS to ensure it lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. For the purpose of this Evaluation Activity the relevant keys are those keys that are relied upon to support any of the SFRs in the Security Target. The evaluator confirms that the description of keys and storage locations is consistent with the functions carried out by the TOE (e.g. that all keys for the TOE-specific secure channels and protocols, or that support FPT_APW.EXT.1 and FPT_SKP_EXT.1, are

	accounted for2). In particular, if a TOE claims not to store plaintext keys in non-volatile memory then the evaluator checks that this is consistent with the operation of the TOE.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS lists all relevant keys (describing the origin and storage location of each), all relevant key destruction situations (e.g. factory reset or device wipe function, disconnection of trusted channels, key change as part of a secure channel protocol), and the destruction method used in each case. Upon investigation, the evaluator found that the TSS lists the keys subject to the destruction requirement in [ST] table Key Zeroization, including the purpose of each key, the storage location (plaintext in RAM, or non-plaintext on CF), and destruction method (single overwrite with zeroes for volatile storage, instruction to destroy the abstraction that represents the key for non-volatile storage) The evaluator examined the [ST] Section 6 to verify that the TSS description of keys and storage locations is consistent with the functions carried out by the TOE. Upon investigation, the evaluator found that the TSS describes all keys associated with SSH and TLS. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.2 FCS_CKM.4 TSS 2

Objective	The evaluator shall check to ensure the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys (e.g., file system APIs, key store APIs).
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS identifies how the TOE destroys keys stored as plaintext in non-volatile memory, and that the description includes identification and description of the interfaces that the TOE uses to destroy keys. Upon investigation, the evaluator found that the TSS states that keys in non-volatile storage are destroyed (via destruction of the abstraction) by the “file delete” command for SSH keys and the “no cak” and “admin save” commands for CAKs. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.3 FCS_CKM.4 TSS 3

Objective	Where the TSS identifies keys that are stored in a non-plaintext form, the evaluator shall check that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS identifies the encryption method and the key-encrypting-key used, and that the key-encrypting-key is either itself stored in an encrypted form or that it is destroyed by a method included under FCS_CKM.4. Upon investigation, the evaluator found that the TSS does not identify any keys stored in non-plaintext form. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.3.4 FCS_CKM.4 TSS 4

Objective	The evaluator shall check that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement (see further discussion in the Guidance Documentation section below). Note that reference may be made to the Guidance Documentation for description of the detail of such cases where destruction may be prevented or delayed.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS identifies any configurations or circumstances that may not conform to the key destruction requirement. Upon investigation, the evaluator found that the TSS does not describe any situation where the key destruction could fail to conform to the requirement. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.5 FCS_CKM.4 TSS 5

Objective	Where the ST specifies the use of "a value that does not contain any CSP" to overwrite keys, the evaluator examines the TSS to ensure that it describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs.
Evaluator Findings	The evaluator examined the [ST] Section 5 to verify that the TSS describes how that pattern is obtained and used, and that this justifies the claim that the pattern does not contain any CSPs. Upon investigation, the evaluator found that the [ST] does not select "a value that does not contain any CSP" Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.3.6 FCS_CKM.4 Guidance 1

Objective	A TOE may be subject to situations that could prevent or delay key destruction in some cases. The evaluator shall check that the guidance documentation identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS (and any other supporting information used). The evaluator shall check that the guidance documentation provides guidance on situations where key destruction may be delayed at the physical layer.
Evaluator Findings	The evaluator examined (AGD) section 6 to verify that it identifies configurations or circumstances that may not strictly conform to the key destruction requirement, and that this description is consistent with the relevant parts of the TSS. Upon investigation, the evaluator found that the AGD does not describe any situation where the key destruction could be prevented or delayed. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4 FCS_COP.1/DataEncryption

5.2.4.1 FCS_COP.1/DataEncryption TSS 1

Objective	The evaluator shall examine the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS to ensure it identifies the key size(s) and mode(s) supported by the TOE for data encryption/decryption. Upon investigation, the evaluator found that the TSS describes support for AES conforming to ISO 18033-3, ISO 10116, and ISO 19772 for CBC, CTR, and GCM modes. [ST] Section 6 states that the TOE supports key sizes of 128 or 256 bits. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.2 FCS_COP.1/DataEncryption Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected mode(s) and key size(s) defined in the Security Target supported by the TOE for data encryption/decryption.
Evaluator Findings	The evaluator examined (AGD) section 7 to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that putting the TOE in CC-NDcPP compliance mode restricts the TOE to only approved key establishment schemes. [AGD] section 3.1 describes how to enable the CC-NDcPP Compliance mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.4.3 FCS_COP.1/DataEncryption Test/CAVP 1

Objective	The evaluator shall verify the implementation of encryption supported by the TOE.
Evaluator Findings	CAVP AES Certs: #C2075, C2084 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5 FCS_COP.1/SigGen

5.2.5.1 FCS_COP.1/SigGen TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the cryptographic algorithm and key size supported by the TOE for signature services.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS to ensure it specifies the cryptographic algorithm and key size supported by the TOE for signature services. Upon investigation, the evaluator found that the TSS describes the use of RSA for SigGen, using key sizes 2048 bits. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.5.2 FCS_COP.1/SigGen Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the selected cryptographic algorithm and key size defined in the Security Target supported by the TOE for signature services.
Evaluator Findings	The evaluator examined (AGD) section 7 to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that putting the TOE in CC-NDcPP compliance mode restricts the TOE to only approved key establishment schemes. [AGD] section 3.1 describes how to enable the CC-NDcPP Compliance mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.5.3 FCS_COP.1/SigGen Test/CAVP 1

Objective	The evaluator shall verify the implementation of signature generation and verification supported by the TOE.
Evaluator Findings	CAVP RSA SigGen&SigVer (186-4) Certs: #C2075, C2084 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6 FCS_COP.1/Hash

5.2.6.1 FCS_COP.1/Hash TSS 1

Objective	The evaluator shall check that the association of the hash function with other TSF cryptographic functions (for example, the digital signature verification function) is documented in the TSS.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS documents the association of the hash function with other TSF cryptographic functions. Upon investigation, the evaluator found that the TSS describes the use of SHA-1, SHA-256, SHA-384, and SHA-512 hashes in support of SSH and TLS, and specified the digest sizes of each hash. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.2 FCS_COP.1/Hash Guidance 1

Objective	The evaluator checks the AGD documents to determine that any configuration that is required to configure the required hash sizes is present.
Evaluator Findings	The evaluator examined (AGD) section 7 to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that putting the TOE in CC-NDcPP compliance mode restricts the TOE to only approved key establishment schemes. [AGD] section 3.1 describes how to enable the CC-NDcPP Compliance mode.

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.6.3 FCS_COP.1/Hash Test/CAVP 1

Objective	The evaluator shall verify the implementation of hashing supported by the TOE.
Evaluator Findings	CAVP SHS Certs: # C2075, C2084 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7 FCS_COP.1/KeyedHash

5.2.7.1 FCS_COP.1/KeyedHash TSS 1

Objective	The evaluator shall examine the TSS to ensure that it specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS specifies the following values used by the HMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS describes the use of HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512, along with their cryptographic parameters. [ST] Section 6 states that keyed hashes are used in support of SSH and TLS sessions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.2 FCS_COP.1/KeyedHash Guidance 1

Objective	The evaluator shall verify that the AGD guidance instructs the administrator how to configure the TOE to use the values used by the HMAC function: key length, hash function used, block size, and output MAC length used defined in the Security Target supported by the TOE for keyed hash function.
Evaluator Findings	The evaluator examined (AGD) section 7 to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that putting the TOE in CC-NDcPP compliance mode restricts the TOE to only approved key establishment schemes. [AGD] section 3.1 describes how to enable the CC-NDcPP Compliance mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.7.3 FCS_COP.1/KeyedHash Test/CAVP 1

Objective	The evaluator shall verify the implementation of MACing supported by the TOE.
Evaluator Findings	CAVP HMAC Certs: # C2075, C2084 Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.2.8 FCS_COP.1(1)/KeyedHashCMAC

5.2.8.1 FCS_COP.1(1)/KeyedHashCMAC TSS 1 **[TD0466]**

Objective	The evaluator shall examine the TSS to ensure that it The evaluator shall examine the TSS to ensure that it specifies the following values used by the AES-CMAC function: key length, hash function used, block size, and output MAC length used.
Evaluator Findings	The evaluator examined [ST] Section 6 to verify that the TSS specifies the following values used by the AES-CMAC function: key length, hash function used, block size, and output MAC length used. Upon investigation, the evaluator found that the TSS describes the key sizes as 128 bits and 256 bits, and the digest size as 128 bits using the AES-CMAC algorithm. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.9 FCS_COP.1(5)

5.2.9.1 FCS_COP.1(5) TSS 1 **[TD0466]**

Objective	The evaluator shall verify that the TSS describes the supported AES modes that are required for this EP in addition to the ones already required by the NDcPP.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the supported AES modes that are required for this EP in addition to the ones already required by the NDcPP. Upon investigation, the evaluator found that the TSS states that the TOE implements AES KeyWrap, AES GCM using cryptographic key sizes of 128 bits or 256 bits against the ISO AES standard (18033-3), AES-KW NIST standard (NIST SP 800-38F), and AES-GCM ISO standard (ISO 19772). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.10 FCS_RBG_EXT.1

5.2.10.1 FCS_RBG_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS specifies the DRBG type, identifies the entropy source(s) seeding the DRBG, and state the assumed or calculated min-entropy supplied either separately by each source or the min-entropy contained in the combined seed value. Upon investigation, the evaluator found that the TSS describes the use of a CTR_DRBG(AES) seeded with 256 bits of entropy. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.10.2 FCS_RBG_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains appropriate instructions for configuring the RNG functionality.
Evaluator Findings	The evaluator examined (AGD) section 7 to verify that it instructs the administrator how to configure the TOE to use the selected key establishment scheme(s). Upon investigation, the evaluator found that the AGD states that putting the TOE in CC-NDcPP compliance mode restricts the TOE to only approved key establishment schemes. [AGD] section 3.1 describes how to enable the CC-NDcPP Compliance mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.10.3 FCS_RBG_EXT.1.1 Test/CAVP 1

Objective	The evaluator shall verify the implementation of SP 800-90A DRBG supported by the TOE.
Evaluator Findings	CAVP DRBG Certs: # C2075, C2084 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (HTTPS)

5.3.1 FCS_HTTPS_EXT.1

5.3.1.1 FCS_HTTPS_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that enough detail is provided to explain how the implementation complies with RFC 2818.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS provides enough detail to explain how the implementation complies with RFC 2818. Upon investigation, the evaluator found that the TSS states that The TOE implements RFC 2818 Section 2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.2 FCS_HTTPS_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to configure TOE for use as an HTTPS client or HTTPS server.
Evaluator Findings	The evaluator examined (AGD) section 4.3 to verify that it described the use of the HTTP client. The TOE uses HTTPS to transfer audit data to the remote audit server, and thus acts as an HTTP client. [AGD] section 4.3 et seq describes configuring the TOE to send audit data to the server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4 TSS and Guidance Activities (SSH)

5.4.1 FCS_SSHS_EXT.1

5.4.1.1 FCS_SSHS_EXT.1.2 TSS 1

Objective	The evaluator shall check to ensure that the TSS contains a description of the public key algorithms that are acceptable for use for authentication and that this list conforms to FCS_SSHS_EXT.1.5. and ensure that if password-based authentication methods have been selected in the ST then these are also described.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSHS_EXT.1.5, and that if password-based authentication methods have been selected in the ST then these are also described. Upon investigation, the evaluator found that the TSS states that the TOE implements the ssh-rsa public key algorithm. The statement in TSS conforms to the selection in FCS_SSHS_EXT.1.5 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.2 FCS_SSHS_EXT.1.3 TSS 1

Objective	The evaluator shall check that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes how “large packets” in terms of RFC 4253 are detected and handled. Upon investigation, the evaluator found that the TSS states that large packets are identified as packets larger than 256kB, and are dropped as described in RFC4253. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.3 FCS_SSHS_EXT.1.4 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the encryption algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the encryption algorithms specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS specifies the optional characteristics and the encryption algorithms supported. Upon investigation, the evaluator found that the TSS states that there are no optional characteristics specified. The description in the TSS conforms to FCS_SSHS_EXT.1.4 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.4 FCS_SSHS_EXT.1.4 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for

	instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).
Evaluator Findings	The evaluator examined (AGD) section 7.1 to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD lists the commands necessary to restrict the SSH implementation to the ciphers defined in [ST]. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.5 FCS_SSHS_EXT.1.5 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics are specified, and the public key algorithms supported are specified as well. The evaluator shall check the TSS to ensure that the public key algorithms specified are identical to those listed for this component.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS specifies the optional characteristics and the public key algorithms supported. Upon investigation, the evaluator found that the TSS states that there are no optional characteristics supported, and the public key algorithm is ssh-rsa. The evaluator verified that the TSS conforms to the selections in FCS_SSHS_EXT.1.5. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.6 FCS_SSHS_EXT.1.5 TSS 2

Objective	The evaluator shall confirm that the TSS includes the description of how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. For example, the TOE could verify that the SSH client's presented public key matches one that is stored within the SSH server's authorized_keys file.
Evaluator Findings	The evaluator examined the [ST] Section 6.3 to verify that the TSS describes how the TOE establishes a user identity when an SSH client presents a public key or X.509v3 certificate. Upon investigation, the evaluator found that the TSS states that the TOE can utilize password-based authentication either with or without an LDAP authentication server, or SSH-RSA public key authentication. TSS states that the TOE compares the presented public_key to an "authorized keys" file stored on the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.7 FCS_SSHS_EXT.1.5 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).

Evaluator Findings	The evaluator examined (AGD) section 6.3 to verify that it contains instructions on configuring the TOE so that SSH conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD describes how to create and install public keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.8 FCS_SSHS_EXT.1.6 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported data integrity algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS lists the supported data integrity algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that the TOE supports hmac-sha1, hmac-sha2-256, hmac-sha2-512, and no others. The Evaluator verified that the TSS conforms to the selections in FCS_SSHS_EXT.1.6. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.9 FCS_SSHS_EXT.1.6 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the “none” MAC algorithm is not allowed).
Evaluator Findings	The evaluator examined (AGD) section 7.1 to verify that it contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD describes how to configure the MAC algorithm. [AGD] section 7.1 does not list the “none” MAC algorithm, or provide instructions to configure it. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.10 FCS_SSHS_EXT.1.7 TSS 1

Objective	The evaluator shall check the TSS to ensure that it lists the supported key exchange algorithms, and that the list corresponds to the list in this component.
Evaluator Findings	The evaluator examined the [ST] Section 7 to verify that the TSS lists the supported key exchange algorithms, and that that list corresponds to the list in this component. Upon investigation, the evaluator found that the TSS states that the TOE supports DH-Group14-sha1, DH-Group14-sha256, and DH-Group16-Sha512 key exchange algorithms. The evaluator verified that the TSS conforms to the selections made in FCS_SSHS_EXT.1.7. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.11 FCS_SSHS_EXT.1.7 Guidance 1

Objective	The evaluator shall also check the guidance documentation to ensure that it contains instructions to the Security Administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE.
Evaluator Findings	The evaluator examined (AGD) section 7.1 to verify that it contains instructions to the administrator on how to ensure that only the allowed key exchange algorithms are used in SSH connections with the TOE. Upon investigation, the evaluator found that the AGD describes how to configure the key-exchange algorithms for SSH. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.12 FCS_SSHS_EXT.1.8 TSS 1

Objective	The evaluator shall check that the TSS specifies the following: a) Both thresholds are checked by the TOE. b) Rekeying is performed upon reaching the threshold that is hit first.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS specifies that both thresholds are checked and that rekeying is performed upon reaching the threshold that is hit first. Upon investigation, the evaluator found that the TSS states that the TOE is capable of rekeying, and that the TOE continuously checks whether either condition (SSH session lasting equal to or longer than 1 hour, ssh session has transmitted more than 1 GB of data) and will initiate a rekey when either threshold is met. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.13 FCS_SSHS_EXT.1.8 Guidance 1

Objective	If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, then the evaluator shall check that the guidance documentation describes how to configure those thresholds. Either the allowed values are specified in the guidance documentation and must not exceed the limits specified in the SFR (one hour of session time, one gigabyte of transmitted traffic) or the TOE must not accept values beyond the limits specified in the SFR. The evaluator shall check that the guidance documentation describes that the TOE reacts to the first threshold reached.
Evaluator Findings	The evaluator examined (AGD) section 3.4 to verify that it describes how to configure any thresholds that are configurable. Upon investigation, the evaluator found that the AGD describes how to configure each threshold. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (TLS)

5.5.1 FCS_TLSC_EXT.1

5.5.1.1 FCS_TLSC_EXT.1.1 TSS 1

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the ciphersuites supported are specified. The evaluator shall check the TSS to ensure that the ciphersuites specified include those listed for this component.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS specifies the ciphersuites supported and that the ciphersuites specified include those listed for this component. Upon investigation, the evaluator found that the TSS lists the supported ciphersuites. The evaluator verified that the list is consistent with the selections made in FCS_TLSC_EXT.1.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.2 FCS_TLSC_EXT.1.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS.
Evaluator Findings	The evaluator examined (AGD) section 7.2 to verify that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS. Upon investigation, the evaluator found that the AGD describes the steps necessary to configure the TOEs TLS implementation and limit it to the ciphersuites selected in the [ST].]. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.3 FCS_TLSC_EXT.1.2 TSS 1

Objective	The evaluator shall ensure that the TSS describes the client's method of establishing all reference identifiers from the administrator/application configured reference identifier, including which types of reference identifiers are supported (e.g. application-specific Subject Alternative Names) and whether IP addresses and wildcards are supported.
Evaluator Findings	The evaluator examined the [ST] Section 7.2 to verify that the TSS describes the client's method of establishing all reference identifiers from the administrator/application-configured reference identifier, including which types of reference identifiers are supported; whether IP addresses and wildcards are supported. Upon investigation, the evaluator found that the TSS states that the TOE verifies that the presented reference identifier matches the reference identifiers. Supported reference identifiers are IPv4 address in SAN, IPv6 address in the SAN, DNS-ID, and CN-ID. TSS states that the TOE does not support wildcards or certificate pinning. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.4 FCS_TLSC_EXT.1.2 TSS 3

Objective	If IP addresses are supported in the CN as reference identifiers, the evaluator shall ensure that the TSS describes the TOE's conversion of the text representation of the IP address in the

	CN to a binary representation of the IP address in network byte order. The evaluator shall also ensure that the TSS describes whether canonical format (RFC 5952 for IPv6, RFC 3986 for IPv4) is enforced.
Evaluator Findings	The evaluator examined the [ST] Section 7 to verify that, if IP addresses are supported in the CN as reference identifiers, the TSS describes the TOE's conversion of the text representation of the IP address in the CN to a binary representation of the IP address in network byte order and whether canonical format is enforced. Upon investigation, the evaluator found that the TSS states that the supported reference identifiers are the SAN, DNS-ID, or CN-ID fields in the presented certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.5 FCS_TLSC_EXT.1.2 Guidance 1

Objective	The evaluator shall ensure that the operational guidance describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not and includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s). If the identifier scheme implemented by the TOE includes support for IP addresses, the evaluator shall ensure that the operational guidance provides a set of warnings and/or CA policy recommendations that would result in secure TOE use.
Evaluator Findings	The evaluator examined (AGD) section 7.2.7 to verify that it describes all supported identifiers, explicitly states whether the TOE supports the SAN extension or not, includes detailed instructions on how to configure the reference identifier(s) used to check the identity of peer(s), and provides a set of warnings and/or CA policy recommendations that would result in secure TOE use. Upon investigation, the evaluator found that the AGD states that the TOE verifies the IPv4, IPv6, and DNS-Name reference identifiers by default, and instructs the administrator on how to configure the expected reference identifier. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.6 FCS_TLSC_EXT.1.2 Guidance 2

Objective	Where the secure channel is being used between components of a distributed TOE for FPT_ITT.1, the SFR selects attributes from RFC 5280, and FCO_CPC_EXT.1.2 selects "no channel"; the evaluator shall verify the guidance provides instructions for establishing unique reference identifiers based on RFC5280 attributes.
Evaluator Findings	The TOE is not distributed. This AA is not applicable Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.7 FCS_TLSC_EXT.1.4 TSS 1

Objective	The evaluator shall verify that TSS describes the Supported Elliptic Curves/Supported Groups Extension and whether the required behaviour is performed by default or may be configured.

Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes the Supported Elliptic Curves Extension and whether the required behaviour is performed by default or may be configured. Upon investigation, the evaluator found that the TSS states that the TOE does not present the supported elliptic curves extension, because no elliptic curves are supported by the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.8 FCS_TLSC_EXT.1.4 Guidance 1

Objective	If the TSS indicates that the Supported Elliptic Curves/Supported Groups Extension must be configured to meet the requirement, the evaluator shall verify that AGD guidance includes configuration of the Supported Elliptic Curves/Supported Groups Extension.
Evaluator Findings	The evaluator examined (AGD) in its entirety along with the [ST] in its entirety to verify that, if the TSS indicates that the Supported Elliptic Curves Extension must be configured to meet the requirement, AGD includes instructions for configuration of the Supported Elliptic Curves Extension. Upon investigation, the evaluator found that [ST] section 6 TSS does not claim support for sending the elliptic curves extension, because no elliptic curves are supported by the TOE, which is consistent with the selections in [ST] section 5.2.2.18. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2 FCS_TLSC_EXT.2

5.5.2.1 FCS_TLSC_EXT.2.1 TSS 1

Objective	The evaluator shall ensure that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS description required per FIA_X509_EXT.2.1 includes the use of client-side certificates for TLS mutual authentication. Upon investigation, the evaluator found that the TSS states that the TOE implements mutually authenticated TLS using X.509v3 certificates. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.2 FCS_TLSC_EXT.2.1 Guidance 1

Objective	If the TSS indicates that mutual authentication using X.509v3 certificates is used, the evaluator shall verify that the AGD guidance includes instructions for configuring the client-side certificates for TLS mutual authentication.
Evaluator Findings	The evaluator examined (AGD) section 7.2 to verify that it includes instructions for configuring the client-side certificates for TLS mutual authentication and the TSS indicates that mutual authentication using X.509v3 certificates is used. Upon investigation, the evaluator found that the AGD describes mutual authentication with external TLS peers, and describes the command to configure mutual-authentication on individual CA profiles.

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (MACsec)

5.6.1 FCS_MACSEC_EXT.1

5.6.1.1 FCS_MACSEC_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the ability of the TSF to implement MACsec in accordance with IEEE 802.1AE-2006.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the ability of the TSF to implement MACsec in accordance with IEEE 802.1AE-2006. Upon investigation, the evaluator found that the TSS states that the TOE implements MACsec in accordance with IEEE Standard 802.1AE-2006, and conforms to IEEE 802.1AE-2006, Sections 5.3a-h, 5.3j-q, 5.4e-h, 8, 9, 10.5,10.6 and 14; IEEE 802.1AEbw-2013 sections 8, 9, 10 and 14 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.2 FCS_MACSEC_EXT.1 TSS 2

Objective	The evaluator shall also determine that the TSS describes the ability of the TSF to derive SCI values from peer MAC address and port data and to reject traffic that does not have a valid SCI.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the ability of the TSF to derive SCI values from peer MAC address and port data and to reject traffic that does not have a valid SCI. Upon investigation, the evaluator found that the TSS states that the TOE receives the SCI based on the port MAC address and sub-port/VLAN ID, from 1 to 1023. TSS also states that the TOE rejects data with an incorrect SCI value. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.1.3 FCS_MACSEC_EXT.1 TSS 3 **[TD0553]**

Objective	The evaluator shall check the TSS for an assertion that only EAPOL, MACsec Ethernet frames, and MAC control frames are accepted by the MACsec interface.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS asserts that only EAPOL and MACsec Ethernet frames and control frames are accepted by the MACsec interface. Upon investigation, the evaluator found that the TSS states that the TOE will only accept EAPOL, MACsec ethernet frames, and MACsec control frames when MAC is enabled on an interface. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2 FCS_MACSEC_EXT.2

5.6.2.1 FCS_MACSEC_EXT.2 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the methods that the TOE implements to provide assurance of MACsec integrity, including the confidentiality offset(s) used, the use of an ICV (including the supported length), and generating the ICV with the SAK, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the methods that the TOE implements to provide assurance of MACsec integrity, including the confidentiality offset(s) used, the use of an ICV (including the supported length), and generating the ICV with the SAK, using the SCI as the most significant bits of the IV and the 32 least significant bits of the PN as the IV. Upon investigation, the evaluator found that the TSS describes the following: An ICV derived with the SAK is used to provide assurance of the integrity of MPDUs, and is 16 octets in length. ICVs are derived from a CAK using KDF, with the SCI as the most significant bits of the IV and the 32 least-significant-bits of the PN as the IV. The ICV is generated in 2 modes: • • With the compliance of 802.1AE, L2 MAC is in clear and all other bytes are encrypted and also part of the ICV calculation. • • When VLAN is clear, 802.1q tags are not the part of the ICV calculation. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2.2 FCS_MACSEC_EXT.2 Guidance 1

Objective	If any integrity verifications are configurable such as the confidentiality offset(s) used or the mechanism used to derive an ICK, the evaluator shall verify that instructions for performing these functions are documented.
Evaluator Findings	The evaluator examined (AGD) section 5 et seq to verify that, if any integrity verifications are configurable such as the confidentiality offset(s) used or the mechanism used to derive an ICK, it documents instructions for performing these functions. Upon investigation, the evaluator found that the AGD (section 5.3.2 step 2 describes configuring AES-128-CMAC or AES-256-CMAC. ([AGD] section 3 states that the TOE must be in FIPS-140-2 mode, which will restrict the cryptographic algorithms to those allowed by the [ST], and [AGD] section 3.1 describes how to put the TOE into FIPS-140-2 mode. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3 FCS_MACSEC_EXT.3

5.6.3.1 FCS_MACSEC_EXT.3 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the method used to generate SAKs and nonces and that the strength of the CAK and the size of the CAK's key space are provided.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the method used to generate SAKs and nonces and that the strength of the CAK and the size of the CAK's key space are provided. Upon investigation, the evaluator found that the TSS states that SAK's are generated using the KeyServer's RNG function, and asserts that no nonces are required because the SAK is not generated using a KDF. TSS states that the CAK is 32 hex characters for the AES-128-CMAC algorithm, or 64 hex characters for the AES-256-CMAC encryption algorithm. TSS also states that SAKs are generated using the Key Server's RNG function. The TOE generates unique Secure Association Keys (SAKs) using key derivation from Connectivity Association Key (CAK) per section 9.8.1 of IEEE 802.1X-2010 such that the likelihood of a repeating SAK is no less than 1 in 2 to the power of the size of the generated key. The TOE generates unique nonce for the derivation of SAKs using the TOE's random bit generator as specified by FCS_RBG_EXT.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4 FCS_MACSEC_EXT.4

5.6.4.1 FCS_MACSEC_EXT.4 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the SAK is wrapped prior to being distributed using the AES implementation specified in this EP.
Evaluator Findings	The evaluator examined [ST] Section 6 to verify that the TSS describes how the SAK is wrapped prior to being distributed using the AES implementation specified. Upon investigation, the evaluator found that the TSS states that the TOE uses AES-KW to distribute SAK's between peers. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4.2 FCS_MACSEC_EXT.4 Guidance 1

Objective	The evaluator shall verify that the guidance provides instructions on how to configure peer authentications. The evaluator shall also verify that the method of specifying a lifetime for CAKs is described.
Evaluator Findings	The evaluator examined (AGD) section 5.3 to verify that it provides instructions on how to configure peer authentications and describes the method of specifying a lifetime for CAKs. Upon investigation, the evaluator found that the AGD section 5.3.2 step 2 describes how to configure a CAK with a pre-shared key and set the encryption modes. Step 11 describes how to configure ports, step 12 describes how to configure sub-ports, step 13 describes how to

	configure the maximum number of peers supported on a specified port. The evaluator also found that section 5.3.3 provides instructions for configuring a CAK lifetime. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5 FCS_MKA_EXT.1

5.6.5.1 FCS_MKA_EXT.1.4 TSS 1

Objective	The evaluator shall examine the TSS to verify that it describes the methods that the TOE implements to provide assurance of MKA integrity, including the use of an ICV and the ability to use a KDF to derive an ICK.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the methods that the TOE implements to provide assurance of MKA integrity, including the use of an ICV and the ability to use a KDF to derive an ICK. Upon investigation, the evaluator found that the TSS states that the TOE derives an ICV from the ICK, which is derived from the CAK by implementing IEEE 802.1X-2010 section 9.3.3 "Derived Keys" using AES-CMAC Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.2 FCS_MKA_EXT.1.8 TSS 1

Objective	The evaluator shall verify that the TSS describes the TOE's compliance with IEEE 802.1X-2010 and 802.1Xbx-2014 for MKA, including the values for MKA and Hello timeout limits and support for data delay protection.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the TOE's compliance with IEEE 802.1X-2010 and 802.1Xbx-2014 for MKA, including the values for MKA and Hello timeout limits and support for data delay protection. Upon investigation, the evaluator found that the TSS states that the TOE implements MKA Lifetime Timeouts limits of 6 to 18 seconds, and a hello Timeout limit of 2 seconds with Hello Timeout configuration values of 500ms, and between 1 to 6 seconds. TSS also states that the TOE implements data delay protection. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.3 FCS_MKA_EXT.1.8 TSS 2

Objective	The evaluator shall also verify that the TSS describes the ability of the PAE of the TOE to establish unique CAs with individual peers and group CAs using a group CAK such that a new group SAK is distributed every time the group's membership changes.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the ability of the PAE of the TOE to establish unique CAs with individual peers and group CAs using a group CAK such that a new group SAK is distributed every time the group's membership changes. Upon investigation, the evaluator found that the TSS states that new SAKs are generated when live peer(s) leave the CA, or a new host joins the CA domain and becomes a member, or when the

	packet number reaches the rollover value 0xc0000000, or when a new PSK is configured and a rollover of PSK has been executed. [ST] asserts that the TOE supports pairwise CAK Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.4 FCS_MKA_EXT.1.8 TSS 3

Objective	The evaluator shall also verify that the TSS describes the invalid MKPDUs that are discarded automatically by the TSF in a manner that is consistent with the SFR, and that valid MKPDUs are decoded in a manner consistent with IEEE 802.1X-2010 section 11.11.4.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the invalid MKPDUs that are discarded automatically by the TSF in a manner that is consistent with the SFR, and that valid MKPDUs are decoded in a manner consistent with IEEE 802.1X-2010 section 11.11.4. Upon investigation, the evaluator found that the TSS describes the circumstances under which the TOE discards KMPDUs. The evaluator verified that this description is consistent with FCS_MKA_EXT.1.8. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.5 FCS_MKA_EXT.1.8 Guidance 1

Objective	The evaluator shall verify that the guidance documentation provides instructions on how to configure the TOE to act as the Key Server in an environment with multiple MACsec-capable devices.
Evaluator Findings	The evaluator examined (AGD) section 5.3.2 to verify that it provides instructions on how to configure the TOE to act as the Key Server in an environment with multiple MACsec-capable devices. Upon investigation, the evaluator found that the AGD describes how to configure "mka-key-server-priority". Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7 TSS and Guidance Activities (Identification and Authentication)

5.7.1 FIA_AFL.1

5.7.1.1 FIA_AFL.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked. The TSS shall also describe the method by which the remote administrator is prevented from successfully logging on to the TOE, and the actions necessary to restore this ability
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS contains a description, for each supported method for remote administrative actions, of how successive unsuccessful authentication attempts are detected and tracked; the method by which the remote administrator is prevented from successfully logging on to the TOE; and the actions necessary

	to restore this ability. Upon investigation, the evaluator found that [ST] section 5.2.3.1 selects "… until an administrator defined time period has elapsed". The TSS states that the security administrator can configure the maximum number of failed attempts for authentication at the CLI as well as the lockout period. The TSS states that the TOE locks the claimed user identity when a user fails to authenticate a number of times equal to the limit. TSS states that locked accounts cannot perform any actions until the lockout period expires. The evaluator verified that the selections in FTP_TRP.1/Admin are consistent with this description (only using the SSH CLI for administrator activity) and are consistent with the TOE architectural description in [ST] section 1, which specifies that the TOE's HTTPS service is used to communicate with the audit server and is not a web GUI. Because the lockout period can be configured by an administrator, and because the expiration of the lockout happens without administrator intervention, it is not necessary that the administrator take any specific action to reenable account access for locked accounts. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.2 FIA_AFL.1 TSS 2

Objective	The evaluator shall examine the TSS to confirm that the TOE ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available, either permanently or temporarily (e.g. by providing local logon which is not subject to blocking).
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS ensures that authentication failures by remote administrators cannot lead to a situation where no administrator access is available. Upon investigation, the evaluator found that the TSS describes that the local access to the TOE is preserved even when an account is locked out. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.3 FIA_AFL.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to ensure that instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented) are provided, and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). If different actions or mechanisms are implemented depending on the secure protocol employed (e.g., TLS vs. SSH), all must be described.
Evaluator Findings	The evaluator examined (AGD) section 6.6 to verify that it provides instructions for configuring the number of successive unsuccessful authentication attempts and time period (if implemented), and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). Upon investigation, the evaluator found that the AGD describes how to configure the lockout duration. [ST] section 5.2.3.1 does not select or assign any behavior that requires administrator action, and [AGD] section 6.6 does not describe administrator actions. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.7.1.4 FIA_AFL.1 Guidance 2

Objective	The evaluator shall examine the guidance documentation to confirm that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1.
Evaluator Findings	The evaluator examined (AGD) section 2.1 to verify that it describes, and identifies the importance of, any actions that are required in order to ensure that administrator access will always be maintained, even if remote administration is made permanently or temporarily unavailable due to blocking of accounts as a result of FIA_AFL.1. Upon investigation, the evaluator found that the AGD states that local access at the TOE console port will always be available even if other methods of access are down, and describes how local access to the TOE is preserved even when an account is locked out. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.1.5 FIA_AFL.1 (MACsec) Guidance 1

Objective	The evaluator shall also examine the operational guidance to ensure that instructions for configuring the authentication failure threshold and the TOE's response to the threshold being met (if configurable), and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). If different actions or mechanisms are implemented depending on the trusted path used to access the TSF (see FTP_TRP.1), all must be described.
Evaluator Findings	The evaluator examined section 6.6 in the AGD to verify that it provides instructions for configuring the authentication failure threshold and the TOE's response to the threshold being met (if configurable), and that the process of allowing the remote administrator to once again successfully log on is described for each "action" specified (if that option is chosen). Upon investigation, the evaluator found that the AGD documents the command for configuring the failure threshold and lockout period. Since the account is automatically re-enabled at the end of the lock-out period, no further action by an administrator is necessary to re-enable an account. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FIA_PMG_EXT.1

5.7.2.1 FIA_PMG_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS contains the lists of the supported special character(s) and minimum and maximum number of charters supported for administrator passwords. Upon investigation, the evaluator found that the TSS describes the

	supported password composition and special characters, and states that the minimum password length is configurable to between 6 and 50 characters. The evaluator verified that the TSS conforms to the selections and assignments in FIA_PMG_EXT.1.1 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2.2 FIA_PMG_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that it: a) identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and b) provides instructions on setting the minimum password length and describes the valid minimum password lengths supported.
Evaluator Findings	The evaluator examined (AGD) section 6.2 to verify that it identifies the characters that may be used in passwords and provides guidance to security administrators on the composition of strong passwords, and provides instructions on setting the minimum password length and describes the valid minimum password lengths supported. Upon investigation, the evaluator found that the AGD lists the characters which may be used, which is exactly consistent with the selections in [ST] section 5.2.3.2. [AGD] section 6.2 states and lists the method of setting the password, setting minimum password length, and states the maximum and minimum "minimum password length" values accepted by the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3 FIA_PSK_EXT.1/MACsec

5.7.3.1 FIA_PSK_EXT.1/MACsec TSS 1

Objective	The evaluator shall examine the TSS to ensure it describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1.
Evaluator Findings	The evaluator examined [ST] sections 5 and 6 to verify that the TSS describes the process by which the bit-based pre-shared keys are generated (if the TOE supports this functionality), and confirm that this process uses the RBG specified in FCS_RBG_EXT.1. Upon investigation, the evaluator found that the [ST] does not select "generate" in FIA_PSK_EXT.1.2. Further, the evaluator found that TSS states that the TOE can accept pre-shared keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.2 FIA_PSK_EXT.1/MACsec Guidance 1

Objective	The evaluator shall examine the operational guidance to determine that it provides guidance to administrators on the composition of strong pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported.

Evaluator Findings	The evaluator examined (AGD) section 5.3.2 to verify that it provides guidance to administrators on the composition of strong pre-shared keys, and (if the selection indicates keys of various lengths can be entered) that it provides information on the range of lengths supported. Upon investigation, the evaluator found that the [AGD] section 5.3.2 step 2 describes the creation of PSKs with 32 or 64 hex characters, depending on the encryption algorithm desired. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.3 FIA_PSK_EXT.1/MACsec Guidance 2

Objective	The evaluator shall confirm the operational guidance contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit-based pre-shared key (or both).
Evaluator Findings	The evaluator examined (AGD) section 5.3.2 to verify that it contains instructions for either entering bit-based pre-shared keys for each protocol identified in the requirement, or generating a bit- based pre-shared key (or both). Upon investigation, the evaluator found that the AGD states that pre-shared keys can be entered directly into the command line. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4 FIA_UIA_EXT.1

5.7.4.1 FIA_UIA_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it describes the logon process for each logon method (local, remote (HTTPS, SSH, etc.)) supported for the product. This description shall contain information pertaining to the credentials allowed/used, any protocol transactions that take place, and what constitutes a “successful logon”.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes the logon process for each logon method supported for the product. Upon investigation, the evaluator found that the TSS states that the login method is the remote SSH CLI or the local console. TSS describes the connection to both local console using RJ45-Db9 cable and remote SSHv2, and states that users must enter a username and password to authenticate locally or remotely. TSS states that the TOE also accepts RSA public key authentication and LDAP authentication using usernames and passwords. [ST] section 6 states that unsuccessful login will result in the administrator being presented with the login page again. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.2 FIA_UIA_EXT.1 TSS 2

Objective	The evaluator shall examine the TSS to determine that it describes which actions are allowed before user identification and authentication. The description shall cover authentication and identification for local and remote TOE administration.

Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes which actions are allowed before user identification and authentication. Upon investigation, the evaluator found that the TSS states that the TOE displays the advisory notice and consent banner prior to login, but does not permit any actions prior to authentication. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.3 FIA_UIA_EXT.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in are described. For each supported the login method, the evaluator shall ensure the guidance documentation provides clear instructions for successfully logging on. If configuration is necessary to ensure the services provided before login are limited, the evaluator shall determine that the guidance documentation provides sufficient instruction on limiting the allowed services.
Evaluator Findings	The evaluator examined (AGD) sections 2, 5, 6, and 7 to verify that it describes any necessary preparatory steps (e.g., establishing credential material such as pre- shared keys, tunnels, certificates, etc.) to logging in. Upon investigation, the evaluator found that the AGD section 2 describes the initial authentication as part of provisioning the device, [AGD] section 6 et seq describes the steps to configure SSH public keys, passwords, and reference identifiers for trusted paths and trusted channels, and [AGD] section 7 describes how to configure the cryptographic protocols use of authentication information. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5 FIA_UAU.7

5.7.5.1 FIA_UAU.7 Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed.
Evaluator Findings	The evaluator examined (AGD) section 2 to verify that it describes any necessary preparatory steps to ensure authentication data is not revealed while entering for each local login allowed. Upon investigation, the evaluator found that the AGD does not describe any necessary preparatory steps necessary to ensure that authentication data is not revealed. [AGD] section 2.1 states that no authentication data are revealed while logging into the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6 FIA_X509_EXT.1/Rev

5.7.6.1 FIA_X509_EXT.1/Rev TSS 1

Objective	The evaluator shall ensure the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in

	FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). It is expected that revocation checking is performed when a certificate is used in an authentication step and when performing trusted updates (if selected). It is not necessary to verify the revocation status of X.509 certificates during power-up self-tests (if the option for using X.509 certificates for self-testing is selected).
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes where the check of validity of the certificates takes place, and that the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied). Upon investigation, the evaluator found that the TSS states that certificate validity checking is performed when a certificate is presented during an authentication step. TSS describes the rules for validation of the extendedKeyUsage field, and the evaluator verified that TSS conforms to the selections and assignments in FIA_X509_ET.1.1/Rev Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6.2 FIA_X509_EXT.1/Rev TSS 2

Objective	The TSS shall describe when revocation checking is performed and on what certificates. If the revocation checking during authentication is handled differently depending on whether a full certificate chain or only a leaf certificate is being presented, any differences must be summarized in the TSS section and explained in the Guidance.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes when revocation checking is performed and on what certificates. Upon investigation, the evaluator found that the TSS states that revocation checking is performed on all certificates that are presented during an authentication step, at the time they are used in authentication. [ST] section 6 also states that verification checks are performed when certificates are loaded onto the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.6.3 FIA_X509_EXT.1/Rev Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trivially satisfied) and describes how certificate revocation checking is performed and on which certificate.
Evaluator Findings	The evaluator examined (AGD) section 6.4 to verify that it describes where the check of validity of the certificates takes place, describes any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE and describes how certificate revocation checking is performed and on which certificate. Upon investigation, the evaluator found that the AGD describes the revocation check during authentication to TLS peers during authentication steps and during initial load-in to the TOE, the rules for validation of extendedKeyUsage fields, and describes the TOE's validation of the entire chain-of-trust to the root CA.

	Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.7 FIA_X509_EXT.2

5.7.7.1 FIA_X509_EXT.2 TSS 1

Objective	The evaluator shall check the TSS to ensure that it describes how the TOE chooses which certificates to use.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that administrators may choose which certificates to use for which connections using "client profiles" Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.7.2 FIA_X509_EXT.2 TSS 2

Objective	The evaluator shall examine the TSS to confirm that it describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. The evaluator shall verify that any distinctions between trusted channels are described. If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes the behaviour of the TOE when a connection cannot be established during the validity check of a certificate used in establishing a trusted channel. Upon investigation, the evaluator found that the TSS states that the TOE will perform revocation checking on certificates if CRL checking is configured. If the TOE is unable to establish a connection to the CRL DP to determine the validity of the certificate, the TOE will not accept the certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.7.3 FIA_X509_EXT.2 Guidance 1

Objective	The evaluator shall check the administrative guidance to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates.
Evaluator Findings	The evaluator examined (AGD) section 6.4 to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD describes the installation of CA certificates, trust chains, and certificate profiles linking specific certificates to specific services and usages of the certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.7.4 FIA_X509_EXT.2 Guidance 2

Objective	If the requirement that the administrator is able to specify the default action, then the evaluator shall ensure that the guidance documentation contains instructions on how this configuration action is performed.
Evaluator Findings	The evaluator examined (AGD) to verify that, if the requirement that the administrator is able to specify the default action, the guidance documentation contains instructions on how this configuration action is performed. Upon investigation, the evaluator found that the [ST] selects only “not accept the certificate” and that the behavior is not configurable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.7.5 FIA_X509_EXT.2 Guidance 3

Objective	The evaluator shall also ensure that the guidance documentation describes the configuration required in the operating environment so the TOE can use the certificates. The guidance documentation shall also include any required configuration on the TOE to use the certificates. The guidance document shall also describe the steps for the Security Administrator to follow if the connection cannot be established during the validity check of a certificate used in establishing a trusted channel.
Evaluator Findings	The evaluator examined (AGD) section 6.4 to ensure that it includes any necessary instructions for configuring the operating environment so that the TOE can use the certificates. Upon investigation, the evaluator found that the AGD describes the installation of CA certificates, trust chains, and certificate profiles linking specific certificates to specific services and usages of the certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.8 FIA_X509_EXT.3

5.7.8.1 FIA_X509_EXT.3 TSS 1

Objective	If the ST author selects "device-specific information", the evaluator shall verify that the TSS contains a description of the device-specific fields used in certificate requests.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS contains a description of the device-specific fields used in certificate requests. Upon investigation, the evaluator found that [ST] does not select “device specific information” in FIA_X509_EXT.3.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.8.2 FIA_X509_EXT.3 Guidance 1

Objective	The evaluator shall check to ensure that the guidance documentation contains instructions on requesting certificates from a CA, including generation of a Certificate Request. If the ST author selects "Common Name", "Organization", "Organizational Unit", or "Country", the

	evaluator shall ensure that this guidance includes instructions for establishing these fields before creating the Certification Request.
Evaluator Findings	The evaluator examined (AGD) section 6.5 to verify that it contains instructions on requesting certificates from a CA, including generation of a Certification Request. Upon investigation, the evaluator found that the AGD describes the required steps to generate a CSR that includes all required information. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8 TSS and Guidance Activities (Security Management)

5.8.1 FMT_MOF.1/ManualUpdate

5.8.1.1 FMT_MOF.1/ManualUpdate Guidance 1

Objective	The evaluator shall examine the guidance documentation to determine that any necessary steps to perform manual update are described. The guidance documentation shall also provide warnings regarding functions that may cease to operate during the update (if applicable).
Evaluator Findings	The evaluator examined (AGD) section 8 to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD describes obtaining the update candidate via out-of-band sources (from the Nokia secure portal), copying the update candidate to a compact-flash drive, and providing the drive to the TOE. [AGD] states that the TOE will search for the update candidate when rebooting or powering on. The evaluator examined (AGD) section 8 to verify that it provides warnings regarding functions that may cease to operate during the update (if applicable). Upon investigation, the evaluator found that the AGD states that there is minimal service interruption, due to requiring the administrator to switch to the updated but “standby” CPM within 3 seconds. By this method, at least one active instance is always-on. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2 FMT_MOF.1/Functions

5.8.2.1 FMT_MOF.1/Functions TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS for each administrative function identified the TSS details how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE).
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that for each administrative function identified the TSS details how the Security Administrator modifies the behaviour of transmitting audit data to an external IT entity. Upon investigation, the evaluator found that

	the TSS states that the TOE restricts the ability to modify the behaviour of transmission of audit data to an audit server to Security Administrators. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2.2 FMT_MOF.1/Functions Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the Security Administrator determines or modifies the behaviour of (whichever is supported by the TOE) transmitting audit data to an external IT entity, handling of audit data, audit functionality when Local Audit Storage Space is full (whichever is supported by the TOE) are performed to include required configuration settings.
Evaluator Findings	The evaluator examined (AGD) section 4 to verify that it describes how the Security Administrator modifies the behaviour of transmitting audit data to an external IT entity. Upon investigation, the evaluator found that the AGD describes the necessary configuration of how frequently the TOE transmits audit data to the server, selecting the server to transmit to. [AGD] section 7.2 describes configuring TLS, including TLS client-profiles for providing the TLS trusted channel to the audit server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3 FMT_MTD.1/CoreData

5.8.3.1 FMT_MTD.1/CoreData TSS 1

Objective	The evaluator shall examine the TSS to determine that, for each administrative function identified in the guidance documentation; those that are accessible through an interface prior to administrator log-in are identified. For each of these functions, the evaluator shall also confirm that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS identifies administrative functions that are accessible through an interface prior to administrator log-in. Upon investigation, the evaluator found that the TSS states that the TOE implements role-based access control, and requires that security administrators log in before they can access any administrative functions. The evaluator examined the [ST] Section 6 to verify that the TSS details how the ability to manipulate the TSF data through these interfaces is disallowed for non-administrative users. Upon investigation, the evaluator found that the TSS states that the TOE implements role-based access control specifying two roles: admin, and user. Administrators may manage the certificates in the TOE's trust store and interact with other TSF data, but users are prevented from doing so by the underlying OS and filesystem Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.2 FMT_MTD.1/CoreData TSS 2

Objective	If the TOE supports handling of X.509v3 certificates and implements a trust store, the evaluator shall examine the TSS to determine that it contains sufficient information to describe how the ability to manage the TOE's trust store is restricted.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that, if the TOE supports handling of X.509v3 certificates and implements a trust store, the TSS contains sufficient information to describe how the ability to manage the TOE's trust store is restricted. Upon investigation, the evaluator found that the TSS states that the TOE does implement a trust store, and that only administrators may manage the certificates in the store. [ST] section 6 states that administrators must be properly authenticated and identified, and that the TOE's Role-Based Access Control restricts access to the trust store and other administrative functions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.3 FMT_MTD.1/CoreData Guidance 1

Objective	The evaluator shall review the guidance documentation to determine that each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP is identified, and that configuration information is provided to ensure that only administrators have access to the functions.
Evaluator Findings	The evaluator examined (AGD) to verify that it identifies each of the TSF-data-manipulating functions implemented in response to the requirements of the cPP. Upon investigation, the evaluator found that the AGD fully describes all administrative actions and commands necessary to operate the TOE. [AGD] section 6.1 describes which TSF-data manipulating functions are restricted to administrators only. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.4 FMT_MTD.1/CoreData Guidance 2

Objective	If the TOE supports handling of X.509v3 certificates and provides a trust store, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. If the TOE supports loading of CA certificates, the evaluator shall review the guidance documentation to determine that it provides sufficient information for the administrator to securely load CA certificates into the trust store. The evaluator shall also review the guidance documentation to determine that it explains how to designate a CA certificate a trust anchor.
Evaluator Findings	The evaluator examined (AGD) sections 7 to verify that, if the TOE supports handling of X.509v3 certificates and provides a trust store, it provides sufficient information for the administrator to configure and maintain the trust store in a secure way. Upon investigation, the evaluator found that the AGD section 7.2 describes how to install root CAs, intermediate CAs, client certificates, and configure certificate-use profiles to determine which trust chains, certificates, and TLS configurations to use for any given TLS connection. The evaluator examined (AGD) section 7 to verify that, if the TOE supports loading of CA certificates, it provides sufficient information for the administrator to securely load CA

	certificates into the trust store and that it explains how to designate a CA certificate a trust anchor. Upon investigation, the evaluator found that the AGD section 7.2.2 describes how to import a root certificate and CRL to the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4 FMT_MTD.1/CryptoKeys

5.8.4.1 FMT_MTD.1/CryptoKeys TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the TSS states that security administrators may modify, generate, and delete the ssh server keys and pre-shared keys for MACsec. TSS states that only security administrators may manage SSH, TLS, and configured X.509v3 certificate keys via the command line. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.2 FMT_MTD.1/CryptoKeys Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed.
Evaluator Findings	The evaluator examined (AGD) section 6 to verify that it lists the keys the Security Administrator is able to manage to include the options available (e.g. generating keys, importing keys, modifying keys or deleting keys) and how that how those operations are performed. Upon investigation, the evaluator found that the AGD describes how SSH keys are managed in [AGD] section 6.3. [AGD] section 6.4 and 6.5 describe generation of keys for TLS. [AGD] section 7 describes how to associate keys/certificates with specific trusted channels. [AGD] section 5 et seq describes how to create or use keys for MACsec, and how subkeys are derived from the pre-shared key. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5 FMT_SMF.1

5.8.5.1 FMT_SMF.1 TSS 1

Objective	The evaluator shall confirm that the TSS details which security management functions are available through which interface(s) (local administration interface, remote administration interface). The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that the TOE can be accessed via local console CLI and remote SSH CLI, and lists the management functions available. The evaluator verified that the TSS description conforms to FMT_SMF.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.5.2 FMT_SMF.1 Guidance 1

Objective	The evaluator shall examine the TSS and Guidance Documentation to verify they both describe the local administrative interface. The evaluator shall ensure the Guidance Documentation includes appropriate warnings for the administrator to ensure the interface is local.
Evaluator Findings	The evaluator examined (AGD) section 2 to verify that it describes the local administrative interface. Upon investigation, the evaluator found that the AGD states that the local administrative interface is the local physical console. The evaluator examined (AGD) section 2 to verify that it includes appropriate warnings for the administrator to ensure the interface is local. Upon investigation, the evaluator found that the AGD states that connection to the local console is performed using the local console cable provided in the box or a standard serial cable with a male DB9 connector, using a baud rate of 115,200, and using a local terminal emulator such as PuTTY. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.6 FMT_SMF.1/MACsec

5.8.6.1 FMT_SMF.1.1/MACsec TSS 1 **[TD0512]**

Objective	The evaluator shall verify that the TSS describes the ability of the TOE to provide the management functions defined in this SFR in addition to the management functions required by the base NDcPP.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes the ability of the TOE to provide the management functions defined in this SFR in addition to the management functions required by the base NDcPP. Upon investigation, the evaluator found that the TSS states that the administrator may perform all functions listed in the SFR. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.8.6.2 FMT_SMF.1.1/MACsec Guidance 1 **[TD0512]**

Objective	The evaluator shall examine the operational guidance to determine that it provides instructions on how to perform each of the management functions defined in this SFR in addition to those required by the base NDcPP.
Evaluator Findings	The evaluator examined (AGD) to verify that it provides instructions on how to perform each of the management functions defined in this SFR in addition to those required by the base NDcPP. Upon investigation, the evaluator found that the SFR requires the administrator to be able to perform the following functions: Generate a PSK and install it in the CAK cache of a device, described in [AGD] section 5.3 and 5.3.2 Manage the Key Server to create, delete, and activate MKA participants as specified in 802.1X, sections 9.13 and 9.16 and section 12.2, described in [AGD] section 5.3.2 for the creation of MKA participants (Step 12), activation of participants (Step 14), and deletion of participants (Step 15). Specify a lifetime of a CAK, described in [AGD] section 5.3.3, and Enable, disable, or delete a PSK-based CAK, described in [AGD] section 5.3.2 Configure the number of failed administrator authentication attempts that will cause an account to be locked out, described in [AGD] section 6.6 Configure the time interval for administrator lockout due to excessive authentication failures, described in [AGD] section 6.6 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.7 FMT_SMR.2

5.8.7.1 FMT_SMR.2 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the TOE supported roles and any restrictions of the roles involving administration of the TOE.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TOE supported roles and any restrictions of the roles involving administration of the TOE. Upon investigation, the evaluator found that the TSS states that the TOE permits the security administrator to configure user privileges individually. TSS states that the TOE implements role-based access control using two roles: admin and user, and that only administrators may interact with TSF data. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.7.2 FMT_SMR.2 Guidance 1

Objective	The evaluator shall review the guidance documentation to ensure that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration.
Evaluator Findings	The evaluator examined (AGD) section 2 to verify that it contains instructions for administering the TOE both locally and remotely, including any configuration that needs to be performed on the client for remote administration. Upon investigation, the evaluator found that the AGD states that the TOE can be administered locally and remotely, and describes how to connect to and authenticate to the TOE via the local console and the remote SSH console. [AGD] section 6.2 describes configuration of passwords. [AGD] section 6.3 describes configuration of SSH public keys. [AGD] section 7.1 describes configuration of the TOE SSH implementation. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9 TSS and Guidance Activities (Protection of the TSF)

5.9.1 FPT_APW_EXT.1

5.9.1.1 FPT_APW_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext password data when stored. The TSS shall also detail passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS details all authentication data that are subject to this requirement and the method used to obscure the plaintext password data when stored. Upon investigation, the evaluator found that the TSS states that all passwords are protected, by storing them as non-reversible hashes in the underlying filesystem in a secure directory. The evaluator also examined the [ST] Section 6 to verify that the TSS details that passwords are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that the storage directory is not readily accessible even to administrators. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2 FPT_CAK_EXT.1

5.9.2.1 FPT_CAK_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how CAKs are stored and that they are unable to be viewed through an interface designed specifically for that purpose. If these values are not stored in plaintext, the TSS shall describe how they are protected or obscured.

Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS details how CAKs are stored and that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that CAKs are stored encrypted by AES-256. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3 FPT_FLS.1(2)/SelfTest

5.9.3.1 FPT_FLS.1(2)/SelfTest TSS 1 **[TD0190]**

Objective	The evaluator shall examine the TSS to determine that it indicates that the TSF will shut down in the event that a self-test failure is detected. For TOEs with redundant failover capability, the evaluator shall examine the TSS to determine that it indicates that the failed components will shut down in the event that a self-test failure is detected.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS indicates that the TSF will shut down in the event that a self-test failure is detected. Upon investigation, the evaluator found that the TSS states that the TOE will reboot, then display diagnostic information at the local console. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.3.2 FPT_FLS.1(2)/SelfTest Guidance 1 **[TD0190]**

Objective	The evaluator shall examine the operational guidance to verify that it describes the behavior of the TOE following a self-test failure and actions that an administrator should take if it occurs.
Evaluator Findings	The evaluator examined [AGD] section 3.2 to verify that the AGD indicates that the TSF will shut down in the event that a self-test failure is detected. Upon investigation, the evaluator found that the AGD states that the TOE will reboot, then display diagnostic information at the local console. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.4 FPT_RPL.1

5.9.4.1 FPT_RPL.1.2 TSS 1

Objective	The evaluator shall examine the TSS to determine that it describes how replay is detected for MPDUs and how replayed MPDUs are handled by the TSF.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that the TSS describes how replay is detected for MPDUs and how replayed MPDUs are handled by the TSF. Upon investigation, the evaluator found that the TSS states that the TOE validates the MKA PDU by size and ICV, then verifies that the message number is greater than the previous message from the peer. If a replay attempt is detected (MKA PDU is invalid, or MessageNumber is less than or equal to the last MN received from the peer, the TOE discards the replayed data, and logs the attempt.

	TSS states that further replay attempts may cause the MKA operational state to be switched to OFF by the TSF, based on the MKA timeout value. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.5 FPT_SKP_EXT.1

5.9.5.1 FPT_SKP_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how any preshared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are protected/obscured.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose. Upon investigation, the evaluator found that the TSS states that all private keys are protected, by storing them in the underlying filesystem in a secure directory that is not accessible by any interface. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.6 FPT_STM_EXT.1

5.9.6.1 FPT_STM_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it lists each security function that makes use of time, and that it provides a description of how the time is maintained and considered reliable in the context of each of the time related functions.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS lists each security function that makes use of time and provides a description of how the time is maintained and considered reliable in the context of each of the time related functions. Upon investigation, the evaluator found that the TSS states that the TOE provides timestamps for audit events, session inactivity, and X.509v3 certificate expiration. Reliable time is provided by the underlying hardware clock. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.6.2 FPT_STM_EXT.1 Guidance 1

Objective	The evaluator examines the guidance documentation to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the guidance documentation instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.
Evaluator Findings	The evaluator examined (AGD) section 9 to verify that it instructs the administrator how to set the time. Upon investigation, the evaluator found that the AGD describes the process for

	setting the time, disabling the unevaluated NTP client, and verifying the system is using the correct time. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.7 FPT_TST_EXT.1.1

5.9.7.1 FPT_TST_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS to ensure that it details the self-tests that are run by the TSF; this description should include an outline of what the tests are actually doing (e.g., rather than saying "memory is tested", a description similar to "memory is tested by writing a value to each memory location and reading it back to ensure it is identical to what was written" shall be used). The evaluator shall ensure that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS details the self-tests that are run by the TSF on start-up. Upon investigation, the evaluator found that the TSS describes the use of integrity tests, cryptographic known-answer tests for each algorithm, and entropy noise source health testing. The evaluator examined the [ST] Section 6 to verify that the TSS makes an argument that the tests are sufficient to demonstrate that the TSF is operating correctly. Upon investigation, the evaluator found that the TSS states that any self test failure will cause the TOE to reboot and display error information at the local console. TSS also states that the TOE does not forward packets on any interface during self-testing, and self-testing only concludes when / if all modules pass. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.7.2 FPT_TST_EXT.1.1 Guidance 1

Objective	The evaluator shall also ensure that the guidance documentation describes the possible errors that may result from such tests, and actions the administrator should take in response; these possible errors shall correspond to those described in the TSS.
Evaluator Findings	The evaluator examined (AGD) section 3.3.2 to verify that it describes the possible errors that may result from such tests, and actions the administrator should take in response. Upon investigation, the evaluator found that the AGD states that the TOE must display the “FIPS-140-2 Power-on-self-test passed” message. [AGD] Section 3.3.2 states that the administrator should reboot if the message does not appear, or contact vendor support. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.8 FPT_TUD_EXT.1

5.9.8.1 FPT_TUD_EXT.1 TSS 1

Objective	The evaluator shall verify that the TSS describe how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the TSS needs to describe how and when the inactive version becomes active. The evaluator shall verify this description.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes how to query the currently active version. Upon investigation, the evaluator found that the TSS states that the current software version may be queried using the “show version” CLI command. The evaluator examined the [ST] Section 5 to verify that the TOE does not select the ability to install an inactive version of software in FPT_TUD_EXT.1.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.8.2 FPT_TUD_EXT.1 TSS 2

Objective	The evaluator shall verify that the TSS describes all TSF software update mechanisms for updating the system firmware and software (for simplicity the term 'software' will be used in the following although the requirements apply to firmware and software). The evaluator shall verify that the description includes a digital signature verification of the software before installation and that installation fails if the verification fails. Alternatively, an approach using a published hash can be used. In this case the TSS shall detail this mechanism instead of the digital signature verification mechanism. The evaluator shall verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS describes all TSF software update mechanisms for updating the system software, includes a digital signature verification of the software before installation and that installation fails if the verification fails. Upon investigation, the evaluator found that the TSS states that the TOE provides the administrator the ability to install updates manually, and perform verification using a published hash. The evaluator examined the [ST] Section 6 to verify that the TSS describes the method by which the digital signature or published hash is verified to include how the candidate updates are obtained, the processing associated with verifying the digital signature or published hash of the update, and the actions that take place for both successful and unsuccessful signature verification or published hash verification. Upon investigation, the evaluator found that the TSS describes the process for obtaining candidates from the Nokia secure portal, including the file with the published hash. TSS describes how the update file is provided to the TOE over compact flash in the standby CPM; how the hash is verified by extracting the file with the hash and comparing the stored value to a computed-on-the-fly hash of the update candidate; and the results of successful and unsuccessful hash validation. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.9.8.3 FPT_TUD_EXT.1 TSS 3

Objective	If the options 'support automatic checking for updates' or 'support automatic updates' are chosen from the selection in FPT_TUD_EXT.1.2, the evaluator shall verify that the TSS explains what actions are involved in automatic checking or automatic updating by the TOE, respectively.
Evaluator Findings	The evaluator examined the [ST] section 5. Upon investigation, the evaluator found that the [ST] does not select "support automatic checking for updates" or "support automatic updates" in FPT_TUD_EXT.1.2. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.8.4 FPT_TUD_EXT.1 TSS 5

Objective	If a published hash is used to protect the trusted update mechanism, then the evaluator shall verify that the trusted update mechanism does involve an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. In particular, authentication as Security Administration according to FMT_MOF.1/ManualUpdate needs to be part of the update process when using published hashes.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS, if a published hash is used to protect the trusted update mechanism, contains a description of how the trusted update mechanism involves an active authorization step of the Security Administrator, and that download of the published hash value, hash comparison and update is not a fully automated process involving no active authorization by the Security Administrator. Upon investigation, the evaluator found that the TSS states that the security administrator must authorize the switch from the "primary" CPM to the "standby" CPM, which will be running the validated update image. Further, because the TOE does not download updates via it's own mechanisms, the security administrator is in full control of the timing, verification, and installation of all update candidates at all times. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.8.5 FPT_TUD_EXT.1 Guidance 1

Objective	The evaluator shall verify that the guidance documentation describes how to query the currently active version. If a trusted update can be installed on the TOE with a delayed activation, the guidance documentation needs to describe how to query the loaded but inactive version.
Evaluator Findings	The evaluator examined (AGD) section 8 to verify that it describes how to query the currently active version and, if a trusted update can be installed on the TOE with a delayed activation, the loaded but inactive version. Upon investigation, the evaluator found that the AGD states

	that the “show version” command may be used to query the currently executing software version. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.8.6 FPT_TUD_EXT.1 Guidance 2

Objective	The evaluator shall verify that the guidance documentation describes how the verification of the authenticity of the update is performed (digital signature verification or verification of published hash). The description shall include the procedures for successful and unsuccessful verification. The description shall correspond to the description in the TSS.
Evaluator Findings	The evaluator examined (AGD) section 8 to verify that it describes how the verification of the authenticity of the update is performed. Upon investigation, the evaluator found that the AGD states that authenticity is provided by a hash verification method. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.8.7 FPT_TUD_EXT.1 Guidance 3

Objective	If a published hash is used to protect the trusted update mechanism, the evaluator shall verify that the guidance documentation describes how the Security Administrator can obtain authentic published hash values for the updates.
Evaluator Findings	The evaluator examined (AGD) section 8 to verify that it describes, if a published hash is used to protect the trusted update mechanism, how the Security Administrator can obtain authentic published hash values for the updates. Upon investigation, the evaluator found that the AGD states that the published hash is included as a file along with the update candidate when received from the Nokia secure portal. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.8.8 FPT_TUD_EXT.1 Guidance 6

Objective	If this was information was not provided in the TSS: If the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the evaluator shall verify that the Guidance Documentation contains a description of how the certificates are contained on the device. The evaluator also ensures that the Guidance Documentation describes how the certificates are installed/updated/selected, if necessary.
Evaluator Findings	The evaluator examined [ST] section 6 to verify that if the ST author indicates that a certificate-based mechanism is used for software update digital signature verification, the TSS contains a description of how the certificates are contained on the device and describes how the certificates are installed/updated/selected. Upon investigation, the evaluator found that the [ST] does not select the use of certificates for trusted update. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.10 TSS and Guidance Activities (TOE Access)

5.10.1 FTA_SSL_EXT.1

5.10.1.1 FTA_SSL_EXT.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details whether local administrative session locking or termination is supported and the related inactivity time period settings.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS identifies whether local administrative session locking or termination is supported and the related inactivity time period settings. Upon investigation, the evaluator found that the TSS states that local administrative sessions are terminated upon reaching the administrator-configured inactivity period timeout value. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.1.2 FTA_SSL_EXT.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period.
Evaluator Findings	The evaluator examined (AGD) section 10 to verify that it states whether local administrative session locking or termination is supported and instructions for configuring the inactivity time period. Upon investigation, the evaluator found that the AGD states that inactive sessions are terminated. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2 FTA_SSL.3

5.10.2.1 FTA_SSL.3 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details the administrative remote session termination and the related inactivity time period.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS identifies administrative remote session termination and the related inactivity time period. Upon investigation, the evaluator found that the TSS states that remote interactive sessions will be terminated after a configurable time interval of inactivity. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.2.2 FTA_SSL.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation includes instructions for configuring the inactivity time period for remote administrative session termination.

Evaluator Findings	The evaluator examined (AGD) section 10 to verify that it includes instructions for configuring the inactivity time period for remote administrative session termination. Upon investigation, the evaluator found that the AGD describes the process for setting the global inactivity period value for both local CLI and remote SSH CLI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.3 FTA_SSL.4

5.10.3.1 FTA_SSL.4 TSS 1

Objective	The evaluator shall examine the TSS to determine that it details how the local and remote administrative sessions are terminated.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS identifies details how the local and remote administrative sessions are terminated. Upon investigation, the evaluator found that the TSS states that the security administrator is able to terminate their own CLI session(s). Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.3.2 FTA_SSL.4 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation states how to terminate a local or remote interactive session.
Evaluator Findings	The evaluator examined (AGD) section 6.7 to verify that it states how to terminate a local or remote interactive session. Upon investigation, the evaluator found that the AGD states that administrative users may end their sessions by using the “logout” command at the local or remote CLI. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.4 FTA_TAB.1

5.10.4.1 FTA_TAB.1 TSS 1

Objective	The evaluator shall check the TSS to ensure that it details each administrative method of access (local and remote) available to the Security Administrator (e.g., serial port, SSH, HTTPS). The evaluator shall check the TSS to ensure that all administrative methods of access available to the Security Administrator are listed and that the TSS states that the TOE is displaying an advisory notice and a consent warning message for each administrative method of access. The advisory notice and the consent warning message might be different for different administrative methods of access and might be configured during initial configuration (e.g. via configuration file).
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS details each administrative method of access available to the Security Administrator and states that the TOE is displaying an advisory notice and consent warning message for each administrative method of access.

	Upon investigation, the evaluator found that the TSS describes two administrative interfaces: local CLI, and remote CLI. For each, TSS asserts that the administrator may customize an advisory notice and consent banner to be displayed at each interface prior to authentication. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.10.4.2 FTA_TAB.1 Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure that it describes how to configure the banner message.
Evaluator Findings	The evaluator examined (AGD) section 11 to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD states that login banners are provided at the local CLI and remote SSH interfaces. [AGD] Section 11.1 describes how to configure the pre-login message. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11 TSS and Guidance Activities (Trusted Path/Channels)

5.11.1 FTP_ITC.1

5.11.1.1 FTP_ITC.1 TSS 1

Objective	The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. The evaluator shall also confirm that all secure communication mechanisms are described in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST.
Evaluator Findings	The evaluator examined the [ST] Sections 5 & 6 to verify that the TSS, for all communications with authorized IT entities identified in the requirement, each secure communication mechanism is identified in terms of the allowed protocols for that IT entity, whether the TOE acts as a server or a client, and the method of assured identification of the non-TSF endpoint. Upon investigation, the evaluator found that the TSS states that the TOE protects communications to an audit server using HTTPS over TLSv1.2, and the TOE protects communications to audit and LDAP servers using TLSv1.2. TSS also asserts that communications between the TOE and the LDAP server use mutually authenticated TLS. [ST] section 5 selects FCS_TLSC_EXT.1 and FCS_TLSC_EXT.2, indicating that the TOE is a TLS client, and not a server. The evaluator examined the [ST] Section 6 to verify that the TSS describes all secure communication mechanisms in sufficient detail to allow the evaluator to match them to the cryptographic protocol Security Functional Requirements listed in the ST. Upon investigation, the evaluator found that the TSS states that the TOE utilizes TLSv1.2 and HTTPS, which are consistent with the inclusion of FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, and FCS_HTTPS_EXT.1. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.11.1.2 FTP_ITC.1 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken.
Evaluator Findings	The evaluator examined (AGD) section 7 to verify that it contains instructions for establishing the allowed protocols with each authorized IT entity, and that it contains recovery instructions should a connection be unintentionally broken. Upon investigation, the evaluator found that the AGD section 7.2 describes how to configure the TLS parameters. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.2 FTP_TRP.1/Admin

5.11.2.1 FTP_TRP.1/Admin TSS 1

Objective	The evaluator shall examine the TSS to determine that the methods of remote TOE administration are indicated, along with how those communications are protected. The evaluator shall also confirm that all protocols listed in the TSS in support of TOE administration are consistent with those specified in the requirement, and are included in the requirements in the ST.
Evaluator Findings	The evaluator examined the [ST] Section 6 to verify that the TSS indicates the methods of remote TOE administration and how those communications are protected. Upon investigation, the evaluator found that the TSS states that the TOE supports SSHv2 for remote administration, and that the remote administrator initiates the connection. The evaluator examined the [ST] Section 6 to verify that the TSS protocols are consistent with those specified in the requirement. Upon investigation, the evaluator found that the TSS states that the TOE utilizes SSHv2, which is consistent with the inclusion of FCS_SSHS_EXT.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.11.2.2 FTP_TRP.1/Admin Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions for establishing the remote administrative sessions for each supported method.
Evaluator Findings	The evaluator examined (AGD) section 2 and 6 to verify that it contains instructions for establishing the remote administrative sessions for each supported method. Upon investigation, the evaluator found that the AGD describes the process for logging into the TOE via SSH, and [AGD] sections 6.3 and 7.1 describe necessary configuration and preparatory steps prior to authentication via SSH. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 Audit

6.1.1 FAU_GEN.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall test the TOE's ability to correctly generate audit records by having the TOE generate audit records for the events listed in the table of audit events and administrative actions listed above. This should include all instances of an event: for instance, if there are several different I&A mechanisms for a system, the FIA_UIA_EXT.1 events must be generated for each mechanism. The evaluator shall test that audit records are generated for the establishment and termination of a channel for each of the cryptographic protocols contained in the ST. If HTTPS is implemented, the test demonstrating the establishment and termination of a TLS session can be combined with the test for an HTTPS session. When verifying the test results, the evaluator shall ensure the audit records generated during testing match the format specified in the guidance documentation, and that the fields in each audit record have the proper entries. Note that the testing here can be accomplished in conjunction with the testing of the security mechanisms directly.
Test Steps & Expected Test Results	• NOTE: This test case is covered by collecting audit records from each applicable test case • In each test case, collect the audit records required by the Protection Profile **The TOE is able to generate audit records for all auditable events required by the Protection Profile.**
Pass/Fail with Explanation	Pass. The audit records associated with each test case were recorded. A comparison of required audit records to the presented audit records was additionally performed. The analyses showed that each required audit record was generated by the TOE. The TOE meets the test requirements.

6.1.2 FAU_STG_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish a session between the TOE and the audit server according to the configuration guidance provided. The evaluator shall then examine the traffic that passes between the audit server and the TOE during several activities of the evaluator's choice designed to generate audit data to be transferred to the audit server. The evaluator shall observe that these data are not able to be viewed in the clear during this transfer, and that they are successfully received by the audit server. The evaluator shall record the particular software (name, version) used on the audit server during testing. The evaluator shall verify that the TOE is capable of transferring audit data to an external audit server automatically without administrator intervention.
Test Steps & Expected Test Results	• Identify the audit software (name and version) used for this test A screenshot of rsyslog showing it's installed version. • Configure the TOE to communicate with an audit server

	A screenshot of the cron configuration that the TOE uses to connect to the external syslog server. • Generate audit events A screenshot of various commands being performed that would generate audit events by the TOE. • Verify with the log that audit logs have been transferred to audit server A screenshot of the generated audit events appearing on the external syslog server • Verify the traffic between the TOE and an audit server is not sent in plaintext. A packet capture showing encrypted packets
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE automatically transferred audit data to an external audit server and the audit data were not sent in plain text. The TOE meets the test requirements.

6.1.3 FAU_STG_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	Test 2: The evaluator shall perform operations that generate audit data and verify that this data is stored locally. The evaluator shall perform operations that generate audit data until the local storage space is exceeded and verifies that the TOE complies with the behaviour defined in FAU_STG_EXT.1.3. Depending on the configuration this means that the evaluator has to check the content of the audit data when the audit data is just filled to the maximum and then verifies that: The existing audit data is overwritten with every new auditable event that should be tracked according to the specified rule (for the option '**overwrite previous audit records**' in FAU_STG_EXT.1.3)
Test Steps & Expected Test Results	• Generate audit data Screenshots of the evaluator executing cron configuration. • Verify the oldest audit record stored locally The TOE generating logs for the command execution that is stored locally on the TOE. • Generate enough additional audit data to overfill the local audit storage A screenshot of the local storage running out of space. • Verify the oldest audit record stored locally is no longer available A screenshot of the local storage showing that it was overwritten.
Pass/Fail with Explanation	Pass. The evaluator verified that TOE generated audit data and verified that the data were stored locally. The evaluator also verified that the TOE overwrote previous audit records when the local storage space exceeded. The TOE meets the test requirements.

6.1.4 FPT_STM_EXT.1 Test #1

Item	Data
Test Assurance Activity	Test 1: If the TOE supports direct **setting of the time by the Security Administrator** then the evaluator uses the guidance documentation to set the time. The evaluator shall then use an available interface to observe that the time was set correctly.
Test Steps & Expected	• Confirm the current time on the TOE A screenshot of the evaluator querying for the time on the TOE.

Test Results	• Set a new time on the TOE A screenshot of the commands used to change the time on the TOE. • Verify that the new time is set A screenshot of the evaluator querying for the new time on the TOE. • Verify that the new time is set via log A screenshot of the logs confirming the time change.
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE supported direct setting of time by the Security Administrator. The TOE meets the test requirements.

6.1.5 FTP_ITC.1 Test #1

Item	Data
Test Assurance Activity	The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps & Expected Test Results	• Configure the TOE to communicate with an audit server A screenshot of the cron configuration that the TOE uses to connect to the external syslog server. • Generate audit events A screenshot of various commands being performed that would generate audit events by the TOE. • Verify the traffic between the TOE and an audit server is not sent in plaintext A packet capture showing encrypted packets • Configure the TOE to communicate with an Authentication (LDAP) server A screenshot of the LDAP configuration on the TOE. • Log into the TOE from a remote CLI connection through SSH with correct credentials via (LDAP) server A screenshot of the remote SSH user logging into the TOE using credentials from LDAP server. • Verify the traffic between the TOE and an authentication server (LDAP) is not sent in plaintext A packet capture showing encrypted packets • Verify that an audit record was generated for the authentication via LDAP A screenshot of audit event generated by the TOE for the authentication via LDAP.
Pass/Fail with Explanation	Pass. The evaluator verified the communication were successful for each protocol with each authorized IT entity (LDAP and audit server). The TOE meets the test requirements.

6.1.6 FTP_ITC.1 Test #2

Item	Data

Test Assurance Activity	For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the guidance documentation to ensure that in fact the communication channel can be initiated from the TOE.
Test Steps & Expected Test Results	• Configure the TOE to communicate with an audit server A screenshot of the cron configuration that the TOE uses to connect to the external syslog server. • Generate audit events A screenshot of various commands being performed that would generate audit events by the TOE. • Verify the communication channel can be initiated from the TOE to an audit server A packet capture showing encrypted communication channel being initiated. • Configure the TOE to communicate with an Authentication (LDAP) server A screenshot of the LDAP configuration on the TOE. • Log into the TOE from a remote CLI connection through SSH with correct credentials via (LDAP) server A screenshot of the remote SSH user logging into the TOE using credentials from LDAP server. • Verify the communication channel can be initiated from the TOE to an authentication (LDAP) server A screenshot of audit event generated by the TOE for the authentication via LDAP.
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE initiated communication for each protocol and verified the connection was successful. The TOE meets the test requirements.

6.1.7 FTP_ITC.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.
Test Steps & Expected Test Results	This test has covered by test FTP_ITC,1 Test #1 where evaluator has verified that for each communication channel with an authorized IT entity, the channel data is sent encrypted.
Pass/Fail with Explanation	Pass. The evaluator verified that for each communication channel with an authorized IT entity (LDAP and audit server), the channel data were encrypted. The TOE meets the test requirements.

6.1.8 FTP_ITC.1 Test #4

Item	Data
Test Assurance Activity	Objective: The objective of this test is to ensure that the TOE reacts appropriately to any connection outage or interruption of the route to the external IT entities. The evaluator shall, for each instance where the TOE acts as a client utilizing a secure communication mechanism with a distinct IT entity, physically interrupt the connection of that IT entity for the following durations:

	1. A duration that exceeds the TOE's application layer timeout setting, 2. A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer. The evaluator shall ensure that, when the physical connectivity is restored, communications are appropriately protected and no TSF data is sent in plaintext. In the case where the TOE is able to detect when the cable is removed from the device, another physical network device (e.g., a core switch) shall be used to interrupt the connection between the TOE and the distinct IT entity. The interruption shall not be performed at the virtual node (e.g., virtual switch) and must be physical in nature.
Test Steps & Expected Test Results	• Configure the TOE to communicate with an audit server A screenshot of the cron configuration that the TOE uses to connect to the external syslog server. • Disconnect physically connection and wait for a duration that exceeds the TOE's application layer timeout setting A screenshot showing an interrupted connection. • Reconnect the TOE and the audit server A screenshot showing connection being reestablished. • Reestablish communications between the TOE and the audit server A screenshot showing connection being reestablished. • Verify communications are protected and no data is sent into plain text A packet capture showing encrypted packets • Configure the TOE to communicate with an audit server A screenshot of the cron configuration that the TOE uses to connect to the external syslog server. • Disconnect physically connection and wait for a duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer A screenshot showing an interrupted connection. • Reconnect the TOE and the audit server A screenshot showing connection being reestablished. • Reestablish communications between the TOE and the audit server A screenshot showing connection being reestablished. • Verify communications are protected and no data is sent into plain text A packet capture showing encrypted packets • Configure the TOE to communicate with an Authentication (LDAP) server A screenshot of the LDAP configuration on the TOE. • Disconnect physically connection and wait for a duration that exceeds the TOE's application layer timeout setting A screenshot showing an interrupted connection. • Reconnect the TOE and the Authentication server A screenshot showing connection being reestablished. • Reestablish communications between the TOE and the Authentication (LDAP) server

	A screenshot showing connection being reestablished. • Verify communications are protected and no data is sent into plain text A packet capture showing encrypted packets • Configure the TOE to communicate with an Authentication (LDAP) server A screenshot of the LDAP configuration on the TOE. • Disconnect physically connection and wait for a duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer A screenshot showing an interrupted connection. • Reconnect the TOE and the Authentication (LDAP) server A screenshot showing connection being reestablished. • Reestablish communications between the TOE and the Authentication (LDAP) server A screenshot showing connection being reestablished. • Verify communications are protected and no data is sent into plain text A packet capture showing encrypted packets
Pass/Fail with Explanation	Pass. The evaluator verified that after the physical connectivity was restored, the communication was appropriately protected and no TSF data were sent in plaintext. The TOE meets the test requirements.

6.2 Auth

6.2.1 FCS_CKM.2 RSA

Item	Data
Test Assurance Activity	**Key Establishment Schemes** The evaluator shall verify the correctness of the TSF's implementation of RSAES-PKCS1-v1_5 by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses RSAES-PKCS1-v1_5. ***TD0580 has been applied.***
Test Steps & Expected Test Results	This test has been successfully tested in FTP_TRP.1/Admin and FTP_ITC.1 because in both SFRs, evaluator has tested each protocol and verified the successful connection.
Pass/Fail with Explanation	Pass. The evaluator verified the correctness of the RSA implementation. The TOE meets the test requirements.

6.2.2 FCS_CKM.2 FCC

Item	Data
Test Assurance Activity	**FFC Schemes using "safe-prime" groups** The evaluator shall verify the correctness of the TSF's implementation of safe-prime groups by using a known good implementation for each protocol selected in FTP_TRP.1/Admin, FTP_TRP.1/Join, FTP_ITC.1 and FPT_ITT.1 that uses safe-prime groups. This test must be performed for each safe-prime group that each protocol uses.
Test Steps & Expected Test Results	This test has been successfully tested in FTP_TRP.1/Admin and FTP_ITC.1 because in both SFRs, evaluator has tested each protocol and verified the successful connection.

Pass/Fail with Explanation	Pass. The evaluator verified the correctness of the FCC implementation. The TOE meets the test requirements.

6.2.3 FIA_AFL.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g., any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE (and, if the time period selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall also use the operational guidance to configure the time period after which access is re-enabled). The evaluator shall test that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.
Test Steps & Expected Test Results	• Configure the TOE to lock out a user after 3 attempts Screenshot of the TOE settings showing that 3 fail login attempts were configured. • Configure the account lockout period length of 3 minutes Screenshot of the TOE settings showing lockout periodof 3 minutes were configured. • Attempt to connect to the TOE from an SSH client using incorrect credentials Screenshot of the 3 attempts to connect to the TOE from an SSH client. • Repeat the failed log-in attempts until the lockout threshold has been met Screenshot of the 4th attempt to connect to the TOE from an SSH client. • Attempt to log into the TOE using correct credentials Screenshot of the 5th attempt to connect to the TOE using correct credentials from an SSH client. • Verify that the login attempt with correct credentials fails Screenshot of the TOE logs confirming the failed attempt. • Verify with the logs that user with incorrect credentials has been locked after reaching the number of successive unsuccessful authentication attempts Screenshot of the TOE logs confirming the failed attempts and lockout.
Pass/Fail with Explanation	Pass. The evaluator verified that once the authentication attempts limit was reached, authentication attempts with valid credentials were no longer successful. The TOE meets the test requirements.

6.2.4 FIA_AFL.1 Test #2b

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE (e.g., any passwords entered as part of establishing the connection protocol or the remote administrator application): Test 2: After reaching the limit for unsuccessful authentication attempts as in Test 1 above, the evaluator shall proceed as follows: If the administrator action selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall confirm by testing that following the operational guidance and performing each action specified in the ST to re-enable the remote administrator's access results in successful access (when using valid credentials for that administrator).

	If the **time period** selection in FIA_AFL.1.2 is included in the ST, then the evaluator shall wait for just less than the time period configured in Test 1 and show that an authorization attempt using valid credentials does not result in successful access. The evaluator shall then wait until just after the time configured in Test 1 and show that an authorization attempt using valid credentials results in successful access.
Test Steps & Expected Test Results	• Attempt to connect to the TOE from an SSH client using incorrect credentials until the lockout threshold of 3 minutes has been met Screenshot of the 3 attempts to connect to the TOE from an SSH client. • Wait a time slightly less than the configured lockout threshold of 3 minutes Screenshot of the 4th attempt to connect to the TOE from an SSH client. • Attempt to log into the TOE using correct credentials Screenshot of the 5th attempt to connect to the TOE using correct credentials from an SSH client. • Verify that the login attempt with correct credentials fail Screenshot of the TOE logs confirming the failed attempt. • Wait a time slightly longer than the configured lockout threshold of 3 minutes and attempt to log into the TOE using correct credentials Screenshot of the 6th attempt to connect to the TOE after waiting longer that lockout threshold of 3 minutes. • Verify using log that the login attempt with correct credentials succeeds Screenshot of the TOE logs confirming the successful login. • Repeat the test steps above for a lockout threshold of 2 minutes
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE did not allow to log in until the time period configured in Test 1 was met and verified that an authorization attempt using valid credentials resulted in successful access after the threshold limit. The TOE meets the test requirements.

6.2.5 FIA_AFL.1 Test #1 (MACsec)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE: Test 1: The evaluator shall use the operational guidance to configure the number of successive unsuccessful authentication attempts allowed by the TOE. The evaluator shall test that once the limit is reached for a given remote administrator account, subsequent attempts with valid credentials are not successful.
Test Steps & Expected Test Results	This test has been covered by FIA_AFL.1 Test #1.
Pass/Fail with Explanation	Pass. This test has been covered by FIA_AFL.1 Test #1.

6.2.6 FIA_AFL.1 Test #3 (MACsec)

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which remote administrators access the TOE:

	Test 3: [conditional] If the TSS indicates that an administrator-configurable time period must elapse in order to automatically re-enable an account that was locked out due to excessive authentication failures, the evaluator shall perform the steps in Test 1 to lock out an account, follow the operational guidance to configure a time period of their choosing, and observe through periodic login attempts that the account cannot successfully log in until the configured amount of time has elapsed. The evaluator shall then repeat this test for a different time period of their choosing.
Test Steps & Expected Test Results	This test has been covered by FIA_AFL.1 Test #2b.
Pass/Fail with Explanation	Pass. This test has been covered by FIA_AFL.1 Test #2b.

6.2.7 FIA_PMG_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall compose passwords that meet the requirements in some way. For each password, the evaluator shall verify that the TOE supports the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that all characters, and a minimum length listed in the requirement are supported and justify the subset of those characters chosen for testing.
Test Steps & Expected Test Results	• Configure the TOE to require a minimum of 6-character passwords Screenshot of the evaluator configuring minimum of 6-character password. • Configure a user with a required password comprised of all Letters (non-repeating) Screenshot of the evaluator attempting to create a password with all letters documented in the TSF. • Configure a user with a required password comprised of all number (may be repeating) Screenshot of the evaluator attempting to create a password with all numbers documented in the TSF. • Configure a user with a required password comprised at least the following “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” Screenshot of the evaluator attempting to create a password with all special characters documented in the TSF. • Configure a user with a 20-character password comprised of any set of characters Screenshot of the evaluator attempting to create a password using allowed 20 characters. • Configure a user with a 30-character password comprised of any set of characters Screenshot of the evaluator attempting to create a password using allowed 30 characters. • Verify that a log was generated for each creation Screenshot of the TOE logging user account creation.
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE supported the password and ensured that all characters, and a minimum length listed in the requirement were supported and justified the subset of those passwords. The TOE meets the test requirements.

6.2.8 FIA_PMG_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall compose passwords that do not meet the requirements in some way. For each password, the evaluator shall verify that the TOE does not support the password. While the evaluator is not required (nor is it feasible) to test all possible compositions of passwords, the evaluator shall ensure that the TOE enforces the allowed characters and the minimum length listed in the requirement and justify the subset of those characters chosen for testing.
Test Steps & Expected Test Results	• Configure the TOE to require a minimum of 6-character passwords Screenshot of the evaluator configuring minimum of 6-character password. • Configure a user with a 1-character password Screenshot of the evaluator configuring 1-character password. • Configure a user a 5-character password Screenshot of the evaluator configuring 5-character password. • Configure a user with a password one more character than the maximum allowed characters Screenshot of the evaluator configuring 57-character password. • Verify that each attempt fails, and a log was generated for each attempt Screenshot of the evaluator being unable to create the passwords.
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE did not support the passwords that did not meet the minimum length requirement and maximum allowed length requirements. The TOE meets the test requirements.

6.2.9 FIA_UIA_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 1: The evaluator shall use the guidance documentation to configure the appropriate credential supported for the login method. For that credential/login method, the evaluator shall show that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access.
Test Steps & Expected Test Results	• Attempt to login from a local connection with incorrect credentials Screenshot of the evaluator attempting to connect to the TOE locally with incorrect credentials. • Confirm that access was denied Screenshot of TOE denying the access. • Verify that an audit record was generated for the authentication attempt Screenshot of TOE generating logs for authentication attempt. • Log into the TOE from a local connection with correct credentials Screenshot of the evaluator attempting to connect to the TOE locally with correct credentials. • Confirm that access was granted Screenshot of TOE allowing the access. • Verify that an audit record was generated for the authentication Screenshot of TOE generating logs for authentication attempt. • Attempt to login from a remote CLI connection through SSH with incorrect credentials

	Screenshot of the evaluator attempting to connect to the TOE through SSH with incorrect credentials. • Confirm that access was denied Screenshot of TOE denying the access. • Verify that an audit record was generated for the authentication attempt Screenshot of TOE generating logs for authentication attempt. • Log into the TOE from a remote CLI connection through SSH with correct credentials Screenshot of the evaluator attempting to connect to the TOE through SSH with correct credentials. • Confirm that access was granted Screenshot of TOE allowing the access. • Verify that an audit record was generated for the authentication Screenshot of TOE generating logs for authentication attempt. • Log into the TOE from a remote CLI connection through SSH with correct credentials using LDAP Screenshot of the evaluator attempting to connect to the TOE with correct credentials using LDAP. • Confirm that access was granted Screenshot of TOE allowing the access. • Verify that an audit record was generated for the authentication Screenshot of TOE generating logs for authentication attempt. • Verify the TOE connection with authentication server is LDAP/TLS using Wireshark A packet capture showing LDAP/TLS connection
Pass/Fail with Explanation	Pass. The evaluator verified every authentication mechanism and the TOE's behavior. The TOE granted the access only when correct credentials were provided and the TOE rejected when user provided incorrect credentials. The TOE meets the test requirements.

6.2.10 FIA_UIA_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 2: The evaluator shall configure the services allowed (if any) according to the guidance documentation, and then determine the services available to an external remote entity. The evaluator shall determine that the list of services available is limited to those specified in the requirement.
Test Steps & Expected Test Results	• Show that commands are not available prior to login (e.g., config, config system, show version, show time, clear) Screenshot of the TOE administrative commands are not available prior to login. • Verify authentication logs reflect failure Screenshot of the TOE logs displaying the failed attempts. • Verify that only the login banner was displayed Screenshot of the login banner displayed prior to login. • Login into the TOE Screenshot of successful login.

	• Show that the previously enabled commands are now available (e.g., config, config system, show version, show time, clear) Screenshot of the TOE administrative commands being available after successful login. • Verify authentication logs reflect success Screenshot of the TOE logs displaying the successful execution of commands.
Pass/Fail with Explanation	Pass. No system services were available to an unauthenticated user who were connecting to the TOE remotely. Only login banner was available. The TOE meets the test requirements.

6.2.11 FIA_UIA_EXT.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall perform the following tests for each method by which administrators access the TOE (local and remote), as well as for each type of credential supported by the login method: Test 3: For local access, the evaluator shall determine what services are available to a local administrator prior to logging in, and make sure this list is consistent with the requirement.
Test Steps & Expected Test Results	• Show that commands are not available prior to login on local CLI (e.g., config, config system, show version, show time, clear) Screenshot of the TOE administrative commands are not available prior to login. • Verify authentication logs reflect failure Screenshot of the TOE logs displaying the failed attempts. • Verify that only the login banner was displayed Screenshot of the login banner displayed prior to login. • Login into the TOE Screenshot of successful login. • Show that the previously enabled commands are now available on local CLI (e.g., config, config system, show version, show time, clear) Screenshot of the TOE administrative commands being available after successful login. • Verify authentication logs reflect success Screenshot of the TOE logs displaying the successful execution of commands.
Pass/Fail with Explanation	Pass. No system services were available to an unauthenticated user who were connecting using locally except the banner. The TOE meets the test requirements.

6.2.12 FIA_UAU.7 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each method of local login allowed: The evaluator shall locally authenticate to the TOE. While making this attempt, the evaluator shall verify that at most obscured feedback is provided while entering the authentication information.

Test Steps & Expected Test Results	• At the directly connected login prompt, enter incorrect authentication credentials Screenshot of the evaluator connecting locally with incorrect credentials. • Verify that at most obscured feedback is provided Screenshot of the TOE displaying obscured or no feedback • At the directly connected login prompt, enter correct authentication credentials Screenshot of the evaluator connecting locally with correct credentials. • Verify that at most obscured feedback is provided Screenshot of the TOE displaying obscured or no feedback
Pass/Fail with Explanation	Pass. The evaluator verified that obscured feedback was provided while entering the authentication information. The TOE meets the test requirements.

6.2.13 FMT_MOF.1/ManualUpdate Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update using a legitimate update image without prior authentication as Security Administrator (either by authentication as a user with no administrator privileges or without user authentication at all – depending on the configuration of the TOE). The attempt to update the TOE shall fail.
Test Steps & Expected Test Results	• At the command prompt, log into the TOE as a user with no administrative privileges Screenshot of the user login with no administrative privileges. • From the unauthenticated command prompt, attempt to execute the commands associated with performing an image update Screenshot of the evaluator running the commands to update the TOE no administrative privileges. • Verify the attempt is unsuccessful Screenshot of the TOE logs displaying failed attempt.
Pass/Fail with Explanation	Pass. The evaluator attempted to update the TOE image without prior authentication as a Security Administrator and verified that the attempt failed. The TOE meets the test requirements.

6.2.14 FMT_MOF.1/ManualUpdate Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform the update with prior authentication as Security Administrator using a legitimate update image. This attempt should be successful. This test case should be covered by the tests for FPT_TUD_EXT.1 already.
Test Steps & Expected Test Results	This test has been covered by FPT_TUD_EXT.1 test #1.
Pass/Fail with Explanation	Pass. This test has been covered by FPT_TUD_EXT.1 test #1. The TOE meets the test requirements.

6.2.15 FMT_MOF.1/Functions (1) Test #1

Item	Data
Test Assurance Activity	Test 1 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for

	configuration of the transmission protocol for transmission of audit data to an external IT entity without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). Attempts to modify parameters without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to modify the security related parameters can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps & Expected Test Results	• Login with a non-administrator account Screenshot of the evaluator attempting to login no administrative privileges. • Attempt to modify parameter related to audit log over TLS Screenshot of the evaluator attempting to modify parameters no administrative privileges. • Show the TOE rejects the modifications Screenshot of the TOE rejecting the modification. • Verify using log that the TOE rejected the modification Screenshot of the TOE logs displaying failed attempt.
Pass/Fail with Explanation	Pass. The TOE did not allow a non-administrator to modify parameters related to the transmission of audit data to an external entity. The TOE meets the test requirements.

6.2.16 MT_MOF.1/Functions (1)Test #2

Item	Data
Test Assurance Activity	Test 2 (if **'transmission of audit data to external IT entity'** is selected from the second selection together with **'modify the behaviour of'** in the first selection): The evaluator shall try to modify all security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The evaluator does not have to test all possible values of the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity but at least one allowed value per parameter.
Test Steps & Expected Test Results	• Login as an administrator Screenshot of the successful login. • Attempt to modify the same parameter as tested in Test #1 Screenshot of the evaluator attempting to modify parameters with administrative privileges. • Show the modifications are successful Screenshot of the TOE allowing the modification. • Verify using log that the TOE allowed the modification Screenshot of the TOE logs displaying successful attempt.
Pass/Fail with Explanation	Pass. The TOE allowed administrator to modify the security parameter related to the transmission of audit data. The TOE meets the test requirements.

6.2.17 FMT_MTD.1/CryptoKeys Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions (modify, delete, generate/import) without prior authentication as Security Administrator (either by authentication as a non-administrative user, if supported, or without authentication at all). Attempts to perform related actions without prior authentication should fail. According to the implementation no other users than the Security Administrator might be defined and without any user authentication the user might not be able to get to the point where the attempt to manage cryptographic keys can be executed. In that case it shall be demonstrated that access control mechanisms prevent execution up to the step that can be reached without authentication as Security Administrator.
Test Steps & Expected Test Results	• Login with a non-administrator account Screenshot of the evaluator attempting to login no administrative privileges. • Attempt to modify parameter related to CAK Screenshot of the evaluator attempting to modify parameters no administrative privileges. • Show the TOE rejects the modifications Screenshot of the TOE rejecting the modification. • Verify using log that the TOE rejected the modification Screenshot of the TOE logs displaying failed attempt.
Pass/Fail with Explanation	Pass. The TOE did not allow to modify the CAK keys when logged in as non-administrator user. The TOE meets the test requirements.

6.2.18 FMT_MTD.1/CryptoKeys Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to perform at least one of the related actions with prior authentication as Security Administrator. This attempt should be successful.
Test Steps & Expected Test Results	• Login with an administrator account Screenshot of the successful login. • Attempt to modify parameter related to CAK Screenshot of the evaluator attempting to modify parameters with administrative privileges. • Show that the TOE allows the modifications Screenshot of the TOE allowing the modification. • Verify using log that the TOE allowed the modification Screenshot of the TOE logs displaying successful attempt.
Pass/Fail with Explanation	Pass. The TOE allowed to modify the CAK when logged in as an administrator. The TOE meets the test requirements.

6.2.19 FMT_SMF.1 Test #1

Item	Data

Test Assurance Activity	The evaluator tests management functions as part of testing the SFRs identified in section 2.4.4. No separate testing for FMT_SMF.1 is required unless one of the management functions in FMT_SMF.1.1 has not already been exercised under any other SFR.
Test Steps & Expected Test Results	All management functions identified in section 2.4.4 have been tested throughout the evaluation. Thus, this requirement has been met. • Generate a table mapping all TOE management functions to specific test cases where these functions are excercised. A table outlining the TOE's management functions and its corresponding test cases will be generated.
Pass/Fail with Explanation	Pass. All management functions identified in section 2.4.4 have been tested throughout the evaluation. The TOE meets the test requirements.

6.2.20 FMT_SMR.2 Test #1

Item	Data
Test Assurance Activity	In the course of performing the testing activities for the evaluation, the evaluator shall use all supported interfaces, although it is not necessary to repeat each test involving an administrative action with each interface. The evaluator shall ensure, however, that each supported method of administering the TOE that conforms to the requirements of this cPP be tested; for instance, if the TOE can be administered through a local hardware interface; SSH; and TLS/HTTPS; then all three methods of administration must be exercised during the evaluation team's test activities.
Test Steps & Expected Test Results	The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces.
Pass/Fail with Explanation	Pass. The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces. The TOE meets the test requirements.

6.2.21 FTA_SSL.3 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.
Test Steps & Expected Test Results	• Configure a remote CLI time out period of 1 minute on administrative sessions Screenshot of the TOE being configured for 1 minute of remote session idle timeout. • Connect to the TOE from the remote CLI Screenshot of the evaluator logging into the TOE using an SSH client. • Verify the time Screenshot of the evaluator verifying the current time on the TOE. • Let the remote CLI connection set idle for 1 minute and verify that the session was terminated Screenshot of TOE's remote session ending after waiting past the timeout expiration. • Verify using log that user has been logged out Screenshot of the TOE generating logs for the events.

	• Configure a remote CLI out period of 2 minutes on administrative sessions Screenshot of the TOE being configured for 2 minute of remote session idle time. • Connect to the TOE from the remote CLI Screenshot of the evaluator logging into the TOE using an SSH client. • Verify the time Screenshot of the evaluator verifying the current time on the TOE. • Let the remote CLI connection set idle for 2 minutes and verify that the session was terminated Screenshot of TOE's remote session ending after waiting past the timeout expiration. • Verify using log that user has been logged out Screenshot of the TOE generating logs for the events.
Pass/Fail with Explanation	Pass. For each time period configured, the evaluator established a remote interactive session with the TOE and then the evaluator observed that the session was terminated after the configured time. The TOE meets the test requirements.

6.2.22 FTA_SSL.4 Test #1

Item	Data
Test Assurance Activity	The evaluator initiates an interactive local session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps & Expected Test Results	• Log onto the TOE through a directly connected interface Screenshot of the evaluator locally logging into the TOE. • Using the instructions provided by the user guide, log off the TOE Screenshot of the evaluator terminating the local session. • Verify with the log that user has logged out Screenshot of the TOE generating logs for the session login and logout.
Pass/Fail with Explanation	Pass. The evaluator initiated an interactive local session with the TOE, logged out the session and observed that the session was terminated. The TOE meets the test requirements.

6.2.23 FTA_SSL.4 Test #2

Item	Data
Test Assurance Activity	The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the guidance documentation to exit or log off the session and observes that the session has been terminated.
Test Steps & Expected Test Results	• Log onto the TOE through remote CLI over SSH Screenshot of the evaluator remotely logging into the TOE. • Using the instructions provided by the user guide, log off the TOE Screenshot of the evaluator terminating the local session. • Verify with the log that user has logged out Screenshot of the TOE generating logs for the session login and logout.

Pass/Fail with Explanation	Pass. The evaluator initiated an interactive remote session with the TOE, logged out the session and observed that the session was terminated. The TOE meets the test requirements.

6.2.24 FTA_SSL_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that reauthentication is needed when trying to unlock the session.
Test Steps & Expected Test Results	• Configure a local time out period of 1 minute on administrative sessions Screenshot of the TOE being configured for 1 minute of session idle timeout. • Connect to the TOE from the local connection Screenshot of the evaluator logging into the TOE locally. • Verify the time Screenshot of the evaluator verifying the current time on the TOE. • Let the local connection set idle for 1 minute and verify that the session was terminated Screenshot of TOE's local session ending after waiting past the timeout expiration. • Verify that a log entry was generated for the session termination Screenshot of the TOE generating logs for the events. • Configure a local time out period of 2 minutes on administrative sessions Screenshot of the TOE being configured for 2 minute of local session idle time. • Connect to the TOE from the local connection Screenshot of the evaluator logging into the TOE locally. • Verify the time Screenshot of the evaluator verifying the current time on the TOE. • Let the local connection set idle for 2 minutes and verify that the session was terminated Screenshot of TOE's local session ending after waiting past the timeout expiration. • Verify that a log entry was generated for the session termination Screenshot of the TOE generating logs for the events.
Pass/Fail with Explanation	Pass. For each time period configured, the evaluator established a local interactive session with the TOE and then observed that the session was terminated after the configured time period. The TOE meets the test requirements.

6.2.25 FTA_TAB.1 Test #1

Item	Data
Test Assurance Activity	The evaluator follows the guidance documentation to configure a notice and consent warning message. The evaluator shall then, for each method of access specified in the TSS, establish a session with the TOE. The evaluator shall verify that the notice and consent warning message is displayed in each instance.

Test Steps & Expected Test Results	• Configure an access banner for each administrative interface Screenshot of the evaluator configuring a local banner for the TOE. • Verify that the administrative access banner is displayed Screenshot of the banner being visible in remote sessions. • Log into the TOE using the local console Screenshot of the evaluator logging into the TOE locally. • Log into the TOE using the remote CLI over SSH Screenshot of the evaluator logging into the TOE using an SSH client. • Verify that the administrative access banner is displayed Screenshot of the banner being visible in remote sessions.
Pass/Fail with Explanation	Pass. The evaluator verified that the notice and consent warning message was displayed in each instance. The TOE meets the test requirements.

6.2.26 FTP_TRP.1/Admin Test #1

Item	Data
Test Assurance Activity	The evaluators shall ensure that communications using each specified (in the guidance documentation) remote administration method is tested during the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps & Expected Test Results	• Initiate a remote CLI connection using SSH with the TOE Screenshot of the evaluator logging into the TOE remotely. • Perform a packet capture and verify that the connection is successful Screenshot of the packet capture showing encrypted packets. • Verify that the connection is connection is successful using logs Screenshot of the TOE generating logs for the successful remote connection.
Pass/Fail with Explanation	Pass. The evaluator verified that remote administration method was tested, and the connection was successful. The TOE meets the test requirements.

6.2.27 FTP_TRP.1/Admin Test #2

Item	Data
Test Assurance Activity	The evaluator shall ensure, for each communication channel, the channel data is not sent in plaintext.
Test Steps & Expected Test Results	• Initiate a remote CLI connection using SSH with the TOE Screenshot of the evaluator logging into the TOE remotely. • Perform a packet capture of the traffic between the TOE and the remote administrator Screenshot of the packet capture showing traffic flow. • Verify that the connection is not sent in plaintext Screenshot of the packet capture showing encrypted packets.
Pass/Fail with Explanation	Pass. The evaluator verified that the channel data were not sent in plaintext. The TOE meets the test requirements.

6.3 SSHS

6.3.1 FCS_SSHS_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	Test 1: If **password-based** authentication methods have been selected in the ST then using the guidance documentation, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that user authentication succeeds when the correct password is provided by the user.
Test Steps & Expected Test Results	• Configure SSH on the TOE Screenshot of the TOE being configured with SSH access. • Verify that an audit log was generated for the configuration Screenshot of the TOE generating logs for the events. • Initiate an SSH connection with the TOE from an SSH client with username/password combination of the SSH user Screenshot of the evaluator logging into the TOE remotely. • Verify that the connection was established by TOE's output using "/show users" command Screenshot of the TOE displaying the active remote users. • Verify that the connection was made by reviewing the TOE Logs Screenshot of the TOE generating logs for the events. • Verify the successful connection with Wireshark Screenshot of the packet capture showing successful connection.
Pass/Fail with Explanation	Pass. The SSH protocol implementation supports the password based authentication when the correct username and password was provided by the user. The TOE meets the test requirements.

6.3.2 FCS_SSHS_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	Test 2: If **password-based** authentication methods have been selected in the ST then the evaluator shall use an SSH client, enter an incorrect password to attempt to authenticate to the TOE, and demonstrate that the authentication fails.
Test Steps & Expected Test Results	• Configure SSH on the TOE Screenshot of the TOE being configured with SSH access. • Initiate an SSH connection with the TOE from an SSH client and provide the correct username and incorrect password Screenshot of the evaluator attempting to log into the TOE remotely. • Verify that the connection was not made by reviewing the TOE logs Screenshot of the TOE logs displaying the failed authentication.
Pass/Fail with Explanation	Pass. The TOE failed password-based authentication when incorrect password was provided for correct username. The TOE meets the test requirements.

6.3.3 FCS_SSHS_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in this component, that packet is dropped.

Test Steps & Expected Test Results	• Establish an SSH connection to the TOE using **Acumen-SSHS** tool Screenshot of the evaluator logging into the TOE remotely using Acumen-SSHS tool. • Verify with the tool output that it sends a packet larger than the established limit Screenshot of the evaluator using the Large Putty tool to send a large packet to the TOE. • Verify with the tool output that the large packet is dropped Screenshot of TOE logs showing that the large packet was dropped. • Verify with the Wireshark output that the large packet is dropped Screenshot of the packet capture showing large packet was dropped.
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE received a packet larger than 256K bytes as specified in this component, and the large packet was dropped. The TOE meets the test requirements.

6.3.4 FCS_SSHS_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator must ensure that only claimed ciphers and cryptographic primitives are used to establish an SSH connection. To verify this, the evaluator shall start session establishment for an SSH connection from a remote client (referred to as 'remote endpoint' below). The evaluator shall capture the traffic exchanged between the TOE and the remote endpoint during protocol negotiation (e.g. using a packet capture tool or information provided by the endpoint, respectively). The evaluator shall verify from the captured traffic that the TOE offers all the ciphers defined in the TSS for the TOE for SSH sessions, but no additional ones compared to the definition in the TSS. The evaluator shall perform one successful negotiation of an SSH session to verify that the TOE behaves as expected. It is sufficient to observe the successful negotiation of the session to satisfy the intent of the test. If the evaluator detects that not all ciphers defined in the TSS for SSH are supported by the TOE and/or the TOE supports one or more additional ciphers not defined in the TSS for SSH, the test shall be regarded as failed.
Test Steps & Expected Test Results	• Configure the TOE to support the ciphers specified in the ST, as follows: • Encryption: aes128-cbc, aes256-cbc, aes128-ctr, aes256-ctr Screenshot of the TOE being configured with listed ciphers. • Connect to the TOE using encryption algorithm aes128-cbc from the SSH client Screenshot of the evaluator remotely connecting to the TOE using the aes128-cbc cipher. • Examine the packet capture and verify that the TOE only presents the encryption algorithm aes128-cbc A packet capture showing that the correct cipher was used. • Verify the connection was made successfully using logs TOE logs showing that the remote connection was successful. • Connect to the TOE using encryption algorithm aes256-cbc from the SSH client Screenshot of the evaluator remotely connecting to the TOE using the aes256-cbc cipher.

	• Examine the packet capture and verify that the TOE only presents the encryption algorithm aes256-cbc A packet capture showing that the correct cipher was used. • Verify the connection was made successfully using logs TOE logs showing that the remote connection was successful. • Connect to the TOE using encryption algorithm aes128-ctr from the SSH client Screenshot of the evaluator remotely connecting to the TOE using the aes128-ctr cipher. • Examine the packet capture and verify that the TOE only presents the encryption algorithm aes128-ctr A packet capture showing that the correct cipher was used. • Verify the connection was made successfully using logs TOE logs showing that the remote connection was successful. • Connect to the TOE using encryption algorithm aes256-ctr from the SSH client Screenshot of the evaluator remotely connecting to the TOE using the aes256-ctr cipher. • Examine the packet capture and verify that the TOE only presents the encryption algorithm aes256-ctr A packet capture showing that the correct cipher was used. • Verify the connection was made successfully using logs TOE logs showing that the remote connection was successful.
Pass/Fail with Explanation	Pass. The TOE only used the claimed ciphers during an SSH connection and made the successful negotiation of the session. The TOE meets the test requirements.

6.3.5 FCS_SSHS_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall establish an SSH connection using each of the public key algorithms specified by the requirement to authenticate the TOE to an SSH client. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.
Test Steps & Expected Test Results	• Generate an SSH keys Screenshot of the evaluator generating an ssh-rsa key-pair. • Configure the TOE SSH implementation to support RSA type of key-based authentication method. Screenshot of the newly created key being imported unto the TOE. • Verify that the TOE generated a log for configuring the SSH client public key TOE logs showing the configuration of the SSH client public key. • Establish an SSH session using ssh-rsa authentication Screenshot of an attempted remote connection to the TOE. • Verify the connection is successful using client output SSH Client logs showing that the remote connection was successful. • Verify the connection is successful using log TOE logs showing that the remote connection was successful. • Verify the connection is successful using packet capture

	A packet capture showing that the successful connection and correct public key algorithm was used.
Pass/Fail with Explanation	Pass. The TOE authenticated a client using the public key authentication based on "ssh-rsa" and made a successful connection. The TOE meets the test requirements.

6.3.6 FCS_SSHS_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	The evaluator shall choose one public key algorithm supported by the TOE. The evaluator shall generate a new key pair for that algorithm without configuring the TOE to recognize the public key for authentication. The evaluator shall use an SSH client to attempt to connect to the TOE with the new key pair and demonstrate that authentication fails. Test objective: The purpose of this negative test is to verify that the server rejects authentication attempts of clients that present a public key that does not match public key(s) associated by the TOE with the identity of the client (i.e. the public keys are unknown to the server). To demonstrate correct functionality, it is sufficient to determine that an SSH connection was not established after using a valid username and an unknown key of supported type.
Test Steps & Expected Test Results	• Re-generate the SSH Key for the SSH client used in FCS_SSHS_EXT.1.5 Test # 1 Screenshot of the evaluator re-generating a new key used in the previous test. • Without uploading the new public key onto the TOE, attempt to log into the TOE using key based authentication Screenshot of an attempted remote connection to the TOE without importing the newly generated key. • Verify through logs that the attempt was unsuccessful TOE logs showing that the connection failed. • Verify through packet capture that the attempt was unsuccessful A packet capture showing that the connection failed.
Pass/Fail with Explanation	Pass. The TOE rejected the authentication attempts of client that presented a public key that did not match public key(s) associated by the TOE with the identity of the client. The TOE meets the test requirements.

6.3.7 FCS_SSHS_EXT.1.5 Test #3

Item	Data
Test Assurance Activity	Test 3: The evaluator shall configure an SSH client to only allow a public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the SSH client to the TOE and observe that the connection is rejected.
Test Steps & Expected Test Results	• Attempt to connect to the TOE from the SSH client configured to only support public key authentication using SSH-DSA Screenshot of the evaluator attempting to remotely connect to the TOE using SSH-DSA key pair. • Verify through client output that the attempt was unsuccessful SSH Client logs showing that the remote connection was unsuccessful. • Verify through logs that the attempt was unsuccessful TOE logs showing that the connection failed.

	• Verify through packet capture that the attempt was unsuccessful A packet capture showing that the connection failed.
Pass/Fail with Explanation	Pass. The SSH connection from the SSH client to the TOE made with "ssh-dss", an unsupported public key algorithm, the TOE rejected the connection. The TOE meets the test requirements.

6.3.8 FCS_SSHS_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	Test 1: [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] The evaluator shall establish an SSH connection using each of the algorithms, except "implicit", specified by the requirement. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. Note: To ensure the observed algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
Test Steps & Expected Test Results	• Configure the TOE to support the MAC algorithms specified in the ST: hmac-sha1, hmac-sha2-256, hmac-sha2-512 Screenshot of the TOE being configured with listed MAC algorithms. • Establish an SSH session to the TOE with hmac-sha1. Screenshot of the evaluator remotely connecting to the TOE using each of the supported MACs. • Verify that user was successfully connected using TOE's "/show users" command output Screenshot of the TOE displaying the active remote users. • Verify that the SSH session was encrypted using the specified MAC using packet capture A packet capture showing the SSH session was encrypted using that the correct mac algorithm was used. • Verify through the TOE's logs that the SSH session was successfully established TOE logs showing that the remote connection was successful. • Establish an SSH session to the TOE with hmac-sha2-256. Screenshot of the evaluator remotely connecting to the TOE using each of the supported MACs. • Verify that user was successfully connected using TOE's "/show users" command output Screenshot of the TOE displaying the active remote users. • Verify that the SSH session was encrypted using the specified MAC using packet capture A packet capture showing the SSH session was encrypted using that the correct mac algorithm was used. • Verify through the TOE's logs that the SSH session was successfully established TOE logs showing that the remote connection was successful. • Establish an SSH session to the TOE with hmac-sha2-512. Screenshot of the evaluator remotely connecting to the TOE using each of the supported MACs.

	• Verify that user was successfully connected using TOE's "/show users" command output Screenshot of the TOE displaying the active remote users. • Verify that the SSH session was encrypted using the specified MAC using packet capture A packet capture showing the SSH session was encrypted using that the correct mac algorithm was used. • Verify through the TOE's logs that the SSH session was successfully established TOE logs showing that the remote connection was successful.
Pass/Fail with Explanation	Pass. The TOE accepted successful connection with claimed MAC algorithms. The TOE meets the test requirements.

6.3.9 FCS_SSHS_EXT.1.6 Test #2

Item	Data
Test Assurance Activity	Test 2: [conditional, if an **HMAC or AEAD_AES_*_GCM** algorithm is selected in the ST] The evaluator shall configure an SSH client to only allow a MAC algorithm that is not included in the ST selection. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails. Note: To ensure the proposed MAC algorithm is used, the evaluator shall ensure a non-aes*-gcm@openssh.com encryption algorithm is negotiated while performing this test.
Test Steps & Expected Test Results	• Configure the TOE to support the MAC algorithms specified in the ST: hmac-sha1, hmac-sha2-256, hmac-sha2-512 Screenshot of the TOE being configured with listed MAC algorithms. • Configure an SSH client to only support HMAC-MD5 and attempt to establish an SSH connection with the TOE Screenshot SSH Client configured to only support HMAC-MD5 and attempting SSH connection. • Verify using client's output that TOE rejected the connection SSH client showing that the connection failed. • Verify that the SSH session was not successful using log TOE logs showing that the connection failed. • Verify that the SSH session was not successful using packet capture A packet capture showing that the connection failed.
Pass/Fail with Explanation	Pass. The SSH connection attempt, using a MAC algorithm that was not supported by the TOE, was rejected. The TOE meets the test requirements.

6.3.10 FCS_SSHS_EXT.1.7 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure an SSH client to only allow the diffie-hellman-group1-sha1 key exchange. The evaluator shall attempt to connect from the SSH client to the TOE and observe that the attempt fails.

Test Steps & Expected Test Results	• Configure the TOE to support the claimed key exchange methods specified in the ST: diffie-hellman-group14- sha1, diffie-hellman-group14-sha256 and diffie-hellman-group16-sha512 Screenshot of the TOE being configured with claimed key exchange methods. • Attempt to connect to the TOE using the SSH client configured to only support diffiehellman-group1-sha1 as the key exchange method Screenshot of the evaluator remotely connecting to the TOE using diffiehellman-group1-sha1. • Verify using Client's output that connection was rejected SSH client showing that the connection was rejected. • Verify using TOE's logs that connection was rejected TOE logs showing that the connection failed. • Verify that the SSH session was not successful using packet capture A packet capture showing that the connection failed.
Pass/Fail with Explanation	Pass. The TOE rejected the SSH connection attempt made by the client using diffie-hellman-group1-sha1 key exchange. The TOE meets the test requirements.

6.3.11 FCS_SSHS_EXT.1.7 Test #2

Item	Data
Test Assurance Activity	For each allowed key exchange method, the evaluator shall configure an SSH client to only allow that method for key exchange, attempt to connect from the client to the TOE, and observe that the attempt succeeds.
Test Steps & Expected Test Results	• Configure the TOE to support the claimed key exchange methods specified in the ST: diffie-hellman-group14- sha1 and diffie-hellman-group14-sha256 and diffie-hellman-group16-sha512 Screenshot of the TOE being configured with claimed key exchange methods. • Establish an SSH session to the TOE diffie-hellman-group14- sha1 Screenshot of the evaluator remotely connecting to the TOE using Diffie-hellman-group14-sha1. • Verify that the SSH session was encrypted using the specified key exchange using packet capture A packet capture showing that the correct key exchange algorithm was used. • Verify through the TOE's logs that the SSH session was successfully established TOE logs showing that the remote connection was successful. • Establish an SSH session to the TOE diffie-hellman-group14-sha256 Screenshot of the evaluator remotely connecting to the TOE using Diffie-hellman-group14-sha256 • Verify that the SSH session was encrypted using the specified key exchange using packet capture A packet capture showing that the correct key exchange algorithm was used. • Verify through the TOE's logs that the SSH session was successfully established TOE logs showing that the remote connection was successful. • Establish an SSH session to the TOE diffie-hellman-group16-sha512 Screenshot of the evaluator remotely connecting to the TOE using Diffie-hellman-group16-sha512

	• Verify that the SSH session was encrypted using the specified key exchange using packet capture A packet capture showing that the correct key exchange algorithm was used. • Verify through the TOE's logs that the SSH session was successfully established TOE logs showing that the remote connection was successful.
Pass/Fail with Explanation	Pass. The SSH connection attempt was successful when the client used allowed key exchange methods that were supported by the TOE. The TOE meets the test requirements.

6.3.12 FCS_SSHS_EXT.1.8 Test #1a

Item	Data
Test Assurance Activity	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the **time-based threshold,** and the traffic-based threshold. For testing of the time-based threshold, the evaluator shall use an SSH client to connect to the TOE and keep the session open until the threshold is reached. The evaluator shall verify that the SSH session has been active longer than the threshold value and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one hour of session time, but the value used for testing shall not exceed one hour. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions).
Test Steps & Expected Test Results	• Configure the TOE to set rekey time limit to 3 minutes Screenshot of the TOE being configured set rekey time limit to 3 minutes. • From an SSH client, establish an SSH connection to the TOE using **Acumen-SSHS** tool Screenshot of the evaluator using the Acumen SSHS tool to establish an SSH connection. • Keep connection alive for a time sufficient to trigger a rekey (note this time cannot be any more than 1 hour) and verify that a rekey was initiated by reviewing the logs on the SSH client Screenshot of SSH client showing that a rekey occurred.
Pass/Fail with Explanation	Pass. The TOE initiated a rekey frequently as per the threshold time value configured on the server. The TOE meets the test requirements.

6.3.13 FCS_SSHS_EXT.1.8 Test #1b

Item	Data
Test Assurance Activity	The evaluator needs to perform testing that rekeying is performed according to the description in the TSS. The evaluator shall test both, the time-based threshold, and the **traffic-based** threshold.

	For testing of the traffic-based threshold the evaluator shall use the TOE to connect to an SSH client and shall transmit data to and/or receive data from the TOE within the active SSH session until the threshold for data protected by either encryption key is reached. It is acceptable if the rekey occurs before the threshold is reached (e.g. because the traffic is counted according to one of the alternatives given in the Application Note for FCS_SSHS_EXT.1.8). The evaluator shall verify that more data has been transmitted within the SSH session than the threshold allows and shall verify that the TOE initiated a rekey (the method of verification shall be reported by the evaluator). Testing does not necessarily have to be performed with the threshold configured at the maximum allowed value of one gigabyte of transferred traffic, but the value used for testing shall not exceed one gigabyte. The evaluator needs to ensure that the rekeying has been initiated by the TOE and not by the SSH client that is connected to the TOE. If one or more thresholds that are checked by the TOE to fulfil the SFR are configurable, the evaluator needs to verify that the threshold(s) can be configured as described in the guidance documentation and the evaluator needs to test that modification of the thresholds is restricted to Security Administrators (as required by FMT_MOF.1/Functions). In cases where data transfer threshold could not be reached due to hardware limitations it is acceptable to omit testing of this (SSH rekeying based on data transfer threshold) threshold if both the following conditions are met: a. An argument is present in the TSS section describing this hardware- based limitation and b. All hardware components that are the basis of such argument are definitively identified in the ST. For example, if specific Ethernet Controller or Wi-Fi radio chip is the root cause of such limitation, these chips must be identified.
Test Steps & Expected Test Results	• Configure the TOE to set rekey data limit to 1024 mb Screenshot of the TOE being configured set rekey data limit to 1024 mb. • From an SSH client, establish an SSH connection to the TOE using the **Acumen-SSHS** tool Screenshot of the evaluator using the Acumen SSHS tool to establish an SSH connection. • Send enough packets to the TOE to cause a rekey (note the total amount of data cannot be more than 1GB to trigger the rekey) Screenshot of SSH client sending enough packets to the TOE to cause a rekey. • Verify that a rekey was initiated by reviewing the SSH client tool output Screenshot of SSH client showing that a rekey occurred.
Pass/Fail with Explanation	Pass. The TOE initiated a rekey as per the data threshold configured on the TOE. The TOE meets the test requirements.

6.4 TLSC

6.4.1 FCS_TLSC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall establish a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of an HTTPS session. It is sufficient to observe the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).
Test Steps & Expected Test Results	• Configure the OpenSSL s_server to use TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 Screenshot of the evaluator configuring remote TLS server to use TLS_RSA_WITH_AES_128_CBC_SHA. • Configure the TOE with cipher TLS_RSA_WITH_AES_128_CBC_SHA Screenshot of the TOE being configured with TLS_RSA_WITH_AES_128_CBC_SHA. • Start a TLS connection from the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify that an audit record was generated for the connection TOE logs showing that the TLS connection was successful. • Verify using packet capture that the selected cipher suite was used A packet capture showing that the TLS connection was successful using the correct cipher. • Configure the OpenSSL s_server to use TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 Screenshot of the evaluator configuring remote TLS server to use TLS_RSA_WITH_AES_256_CBC_SHA. • Configure the TOE with cipher TLS_RSA_WITH_AES_256_CBC_SHA Screenshot of the TOE being configured with TLS_RSA_WITH_AES_256_CBC_SHA. • Start a TLS connection from the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify that an audit record was generated for the connection TOE logs showing that the TLS connection was successful. • Verify using packet capture that the selected cipher suite was used A packet capture showing that the TLS connection was successful using the correct cipher. • Configure the OpenSSL s_server to use TLS_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246 Screenshot of the evaluator configuring remote TLS server to use TLS_RSA_WITH_AES_256_CBC_SHA. • Configure the TOE with cipher TLS_RSA_WITH_AES_128_CBC_ SHA256 Screenshot of the TOE being configured with TLS_RSA_WITH_AES_256_CBC_SHA. • Start a TLS connection from the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify that an audit record was generated for the connection TOE logs showing that the TLS connection was successful.

	• Verify using packet capture that the selected cipher suite was used A packet capture showing that the TLS connection was successful using the correct cipher. • Configure the OpenSSL s_server to use TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246 Screenshot of the evaluator configuring remote TLS server to use TLS_RSA_WITH_AES_128_CBC_ SHA256. • Configure the TOE with cipher TLS_RSA_WITH_AES_256_CBC_ SHA256 Screenshot of the TOE being configured with TLS_RSA_WITH_AES_128_CBC_ SHA256. • Start a TLS connection from the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify that an audit record was generated for the connection TOE logs showing that the TLS connection was successful. • Verify using packet capture that the selected cipher suite was used A packet capture showing that the TLS connection was successful using the correct cipher.
Pass/Fail with Explanation	Pass. The TOE connected to a remote TLS server using the claimed cipher suites. The TOE meets the test requirements.

6.4.2 FCS_TLSC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall attempt to establish the connection using a server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field and verify that a connection is established. The evaluator will then verify that the client rejects an otherwise valid server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field, and a connection is not established. Ideally, the two certificates should be identical except for the extendedKeyUsage field.
Test Steps & Expected Test Results	Part 1 • Attempt to establish the connection using a TLS server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field. Screenshot of the evaluator configuring remote TLS server to use server with a server certificate that contains the Server Authentication purpose in the extendedKeyUsage field. • Attempt a TLS connection from the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the TLS server. • Verify the connection was successful using log TOE logs showing that the TLS connection was successful. • Verify the connection was successful using packet capture A packet capture showing that the TLS connection was successful. Part 2 • Attempt to establish the connection using a TLS server with a server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field.

	Screenshot of the evaluator configuring remote TLS server to use server with a server certificate that lacks the Server Authentication purpose in the extendedKeyUsage field. • Attempt a TLS connection from the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the TLS server. • Verify the connection was not successful using log TOE logs showing that the TLS connection was not successful. • Verify the connection was not successful using packet capture A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The TOE rejected an otherwise valid server certificate that lacked the Server Authentication purpose in the extendedKeyUsage field, and the connection was not established. The TOE meets the test requirements.

6.4.3 FCS_TLSC_EXT.1.1 Test #3

Item	Data
Test Assurance Activity	The evaluator shall send a server certificate in the TLS connection that the does not match the server-selected ciphersuite (for example, send a ECDSA certificate while using the TLS_RSA_WITH_AES_128_CBC_SHA ciphersuite). The evaluator shall verify that the TOE disconnects after receiving the server's Certificate handshake message.
Test Steps & Expected Test Results	• Configure Acumen-TLSC tool to send a server certificate in the TLS connection that the does not match the server-selected ciphersuite Screenshot of Acumen-TLSC tool sending server certificate with mismatched ciphersuite. • Attempt a TLS connection from the TOE to the Acumen-TLSC server Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection was not successful using log TOE logs showing that the TLS connection was not successful. • Verify the connection was not successful using packet capture A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The TOE disconnected the TLS connection after receiving the server's Certificate handshake message. The TLS server was using a certificate that did not match the TOE's cipher suite. The TOE meets the test requirements.

6.4.4 FCS_TLSC_EXT.1.1 Test #4a

Item	Data
Test Assurance Activity	The evaluator shall configure the server to select the TLS_NULL_WITH_NULL_NULL ciphersuite and verify that the client denies the connection.
Test Steps & Expected Test Results	• The evaluator used the Acumen TLSC tool to present a TLS_NULL_WITH_NULL_NULL ciphersuite and verified that the connection was not successful. Screenshot of Acumen-TLSC tool sending server hello with TLS_NULL_WITH_NULL_NULL. • Attempt a TLS connection from the TOE to the Acumen-TLSC server

	Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection was not successful using log TOE logs showing that the TLS connection was not successful. • The evaluator verified the packet capture to ensure that the client denied the connection. A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The TOE denied the connection to the TLS server that was using a NULL ciphersuite. The TOE meets the test requirements.

6.4.5 FCS_TLSC_EXT.1.1 Test #4b

Item	Data
Test Assurance Activity	Modify the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message. The evaluator shall verify that the client rejects the connection after receiving the Server Hello.
Test Steps & Expected Test Results	• The evaluator modified the server's selected ciphersuite in the Server Hello handshake message to be a ciphersuite not presented in the Client Hello handshake message using the Acumen-TLSC tool. Screenshot of Acumen-TLSC tool sending server hello with unsupported ciphersuite. • Attempt a TLS connection from the TOE to the Acumen-TLSC server Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection was not successful using log TOE logs showing that the TLS connection was not successful. • Verify the connection was not successful using packet capture A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The TOE rejected the connection when modified cipher suite was presented in Server Hello handshake message. The TOE meets the test requirements.

6.4.6 FCS_TLSC_EXT.1.1 Test #5a

Item	Data
Test Assurance Activity	Change the TLS version selected by the server in the Server Hello to a non-supported TLS version and verify that the client rejects the connection.
Test Steps & Expected Test Results	• The evaluator attempted a connection to a server using a non-supported TLS version (TLS version 1.0) using Acumen-TLSC tool Screenshot of Acumen-TLSC tool sending server hello with unsupported TLS version. • Attempt a TLS connection from the TOE to the Acumen-TLSC server Screenshot of the TOE initiating a TLS connection to the server. • The evaluator verified the packet capture to ensure that the TOE rejected the connection. A packet capture showing that the TLS connection was not successful. • The evaluator verified that the log indicated an error with handshakeFailure TOE logs showing that the TLS connection was not successful.

Pass/Fail with Explanation	Pass. The TOE rejected the connection request made that was using a non-supported TLS version. The TOE meets the test requirements.

6.4.7 FCS_TLSC_EXT.1.1 Test #5b

Item	Data
Test Assurance Activity	[conditional]: If **using DHE or ECDH**, modify the signature block in the Server's Key Exchange handshake message, and verify that the handshake does not finished successfully, and no application data flows. This test does not apply to cipher suites using RSA key exchange. If a TOE only supports RSA key exchange in conjunction with TLS, then this test shall be omitted.
Test Steps & Expected Test Results	N/A – TOE only supports RSA key exchange in conjunction with TLS.
Pass/Fail with Explanation	N/A – The TOE only supports RSA key exchange in conjunction with TLS.

6.4.8 FCS_TLSC_EXT.1.1 Test #6a

Item	Data
Test Assurance Activity	Modify a byte in the Server Finished handshake message and verify that the handshake does not finish successfully, and no application data flows.
Test Steps & Expected Test Results	• Configure Acumen-TLSC tool to modify a byte in the Server Finished handshake message Screenshot of Acumen-TLSC tool sending modified byte in Server Finished handshake message. • Attempt a TLS connection from the TOE to the Acumen-TLSC server Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection was not successful using log TOE logs showing that the TLS connection was not successful. • Verify the connection was not successful using packet capture A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The evaluator verified that the handshake did not finish successfully, and no application data was sent when a byte was modified in the Server Finished handshake message. The TOE meets the test requirements.

6.4.9 FCS_TLSC_EXT.1.1 Test #6b

Item	Data
Test Assurance Activity	Send a garbled message from the server after the server has issued the ChangeCipherSpec message and verify that the handshake does not finish successfully, and no application data flows.
Test Steps & Expected Test Results	• Configure Acumen-TLSC tool to send a garbled message from the server after the server has issued the ChangeCipherSpec message Screenshot of Acumen-TLSC tool sending a garbled message from the server after the server has issued the ChangeCipherSpec message. • Attempt a TLS connection from the TOE to the Acumen-TLSC server

	Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection was not successful using log TOE logs showing that the TLS connection was not successful. • Verify the connection was not successful using packet capture A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The evaluator verified that the handshake did not finish successfully, and no application data was sent. The TOE meets the test requirements.

6.4.10 FCS_TLSC_EXT.1.1 Test #6c

Item	Data
Test Assurance Activity	Modify at least one byte in the server's nonce in the Server Hello handshake message and verify that the client rejects the Server Key Exchange handshake message (if using a DHE or ECDHE ciphersuite) or that the server denies the client's Finished handshake message.
Test Steps & Expected Test Results	• Configure Acumen-TLSC tool to modify one byte in the server's nonce in the Server Hello handshake message Screenshot of Acumen-TLSC tool sending modified byte in the server's nonce in Server Finished handshake message. • Attempt a TLS connection from the TOE to the Acumen-TLSC server Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection was not successful using log TOE logs showing that the TLS connection was not successful. • Verify the connection was not successful using packet capture A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The evaluator attempted a connection from the TOE to a server running a TLS tool capable of modifying bytes in the server's nonce in the Server Hello handshake message and verified that the TOE rejected the Server Key Exchange handshake message. The TOE meets the test requirements.

6.4.11 FCS_TLSC_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the CN. Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 1.

Test Steps & Expected Test Results	Part 1 - IPv4 • Create a certificate with incorrect CN and missing SAN Screenshot showing certificate with incorrect CN and missing SAN • Start the TLS server with certificate which has incorrect CN and missing SAN Screenshot of the evaluator configuring TLS server to use the invalid cert • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was rejected TOE logs showing that the TLS connection was not successful. • Verified with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful. Part 2 – IPv6 • Create a certificate with incorrect CN and missing SAN Screenshot showing certificate with incorrect CN and missing SAN • Start the TLS server with certificate which has incorrect CN and missing SAN Screenshot of the evaluator configuring TLS server to use the invalid cert • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was rejected TOE logs showing that the TLS connection was not successful. • Verified with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful. Part 3 – DNS-ID • Create a certificate with incorrect CN and missing SAN Screenshot showing certificate with incorrect CN and missing SAN • Start the TLS server with certificate which has incorrect CN and missing SAN Screenshot of the evaluator configuring TLS server to use the invalid cert • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was rejected TOE logs showing that the TLS connection was not successful. • Verified with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The evaluator has verified that TOE rejected the connection when SAN extension was not presented with incorrect CN. The TOE meets the test requirements.

6.4.12 FCS_TLSC_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that

	matches the reference identifier. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, URI). When testing IPv4 or IPv6 addresses, the evaluator shall modify a single decimal or hexadecimal digit in the SAN.
Test Steps & Expected Test Results	Part 1 - IPv4 • Create a certificate with correct CN and incorrect SAN Screenshot showing certificate with correct CN and incorrect SAN • Start the TLS server with certificate which has correct CN and incorrect SAN Screenshot of the evaluator configuring TLS server to use the invalid cert • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was rejected TOE logs showing that the TLS connection was not successful. • Verified with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful. Part 2 – IPv6 • Create a certificate with correct CN and incorrect SAN Screenshot showing certificate with correct CN and incorrect SAN • Start the TLS server with certificate which has correct CN and incorrect SAN Screenshot of the evaluator configuring TLS server to use the invalid cert • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was rejected TOE logs showing that the TLS connection was not successful. • Verified with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful. Part 3 – DNS-ID • Create a certificate with correct CN and incorrect SAN Screenshot showing certificate with correct CN and incorrect SAN • Start the TLS server with certificate which has correct CN and incorrect SAN Screenshot of the evaluator configuring TLS server to use the invalid cert • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was rejected TOE logs showing that the TLS connection was not successful. • Verified with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The evaluator has presented a server certificate that contains a CN that matches the reference identifier, contains the SAN extension, but does not contain an identifier in the SAN that matches the reference identifier and verified that the connection failed. The evaluator has repeated this test for each supported SAN type. The TOE meets the test requirements.

6.4.13 FCS_TLSC_EXT.1.2 Test #3

Item	Data

Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** If the TOE does not mandate the presence of the SAN extension, the evaluator shall present a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each identifier type (e.g. IPv4, IPv6, FQDN) supported in the CN. If the TOE does mandate the presence of the SAN extension, this Test shall be omitted.
Test Steps & Expected Test Results	Part 1 - IPv4 • Create a certificate with correct CN and missing SAN Screenshot showing certificate with correct CN and missing SAN • Start the TLS server with certificate which has correct CN and missing SAN Screenshot of the evaluator configuring TLS server to use the cert with correct CN and missing SAN • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify with log that connection was successful. TOE logs showing that the TLS connection was successful. • Verify with Wireshark that connection was successful. A packet capture showing that the TLS connection was successful. Part 2 – IPv6 • Create a certificate with correct CN and missing SAN Screenshot showing certificate with correct CN and missing SAN • Start the TLS server with certificate which has correct CN and missing SAN Screenshot of the evaluator configuring TLS server to use the cert with correct CN and missing SAN • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify with log that connection was successful. TOE logs showing that the TLS connection was successful. • Verify with Wireshark that connection was successful. A packet capture showing that the TLS connection was successful. Part 3 – DNS-ID • Create a certificate with correct CN and missing SAN Screenshot showing certificate with correct CN and missing SAN • Start the TLS server with certificate which has correct CN and missing SAN Screenshot of the evaluator configuring TLS server to use the cert with correct CN and missing SAN • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify with log that connection was successful. TOE logs showing that the TLS connection was successful. • Verify with Wireshark that connection was successful. A packet capture showing that the TLS connection was successful.

Pass/Fail with Explanation	Pass. The evaluator has presented a server certificate that contains a CN that matches the reference identifier and does not contain the SAN extension and verified that the connection succeeds. The evaluator has repeated this test for each supported CN type. The TOE meets the test requirements.

6.4.14 FCS_TLSC_EXT.1.2 Test #4

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** The evaluator shall present a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches. The evaluator shall verify that the connection succeeds. The evaluator shall repeat this test for each supported SAN type (e.g. IPv4, IPv6, FQDN, SRV).
Test Steps & Expected Test Results	Part 1 - IPv4 • Create a certificate with incorrect CN and valid SAN Screenshot showing certificate with incorrect CN and valid SAN • Start the TLS server with certificate which has incorrect CN and valid SAN • Screenshot of the evaluator configuring TLS server to use the cert with incorrect CN and valid SAN • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was successful. TOE logs showing that the TLS connection was successful. • Verified with Wireshark that connection was successful. A packet capture showing that the TLS connection was successful. Part 2 – IPv6 • Create a certificate with incorrect CN and valid SAN Screenshot showing certificate with incorrect CN and valid SAN • Start the TLS server with certificate which has incorrect CN and valid SAN • Screenshot of the evaluator configuring TLS server to use the cert with incorrect CN and valid SAN • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was successful. TOE logs showing that the TLS connection was successful. • Verified with Wireshark that connection was successful. A packet capture showing that the TLS connection was successful. Part 3 – CN-ID • Create a certificate with incorrect CN and valid SAN Screenshot showing certificate with incorrect CN and valid SAN • Start the TLS server with certificate which has incorrect CN and valid SAN • Screenshot of the evaluator configuring TLS server to use the cert with incorrect CN and valid SAN

	• Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was successful. TOE logs showing that the TLS connection was successful. • Verified with Wireshark that connection was successful. A packet capture showing that the TLS connection was successful. Part 4 – DNS-ID • Create a certificate with incorrect CN and valid SAN Screenshot showing certificate with incorrect CN and valid SAN • Start the TLS server with certificate which has incorrect CN and valid SAN • Screenshot of the evaluator configuring TLS server to use the cert with incorrect CN and valid SAN • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was successful. TOE logs showing that the TLS connection was successful. • Verified with Wireshark that connection was successful. A packet capture showing that the TLS connection was successful.
Pass/Fail with Explanation	Pass. The evaluator has presented a server certificate that contains a CN that does not match the reference identifier but does contain an identifier in the SAN that matches and verified that the connection succeeds. The TOE meets the test requirements.

6.4.15 FCS_TLSC_EXT.1.2 Test #5 (1)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard that is not in the left-most label of the presented identifier (e.g. foo.*.example.com) and verify that the connection fails.
Test Steps & Expected Test Results	• Create a certificate containing a wildcard that is not in the left-most label of the presented identifier as CN-ID with DNS Screenshot showing certificate containing a wildcard that is not in the left-most label of the presented identifier as CN-ID with DNS. • Start TLS server with certificate containing a wildcard that is not in the left-most label of the presented identifier Screenshot of the evaluator configuring TLS server to use the invalid cert. • Attempt the connection from TOE to the TLS server using reference identifier Screenshot of the TOE initiating a TLS connection to the server. • Verify with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful. • Verify with log that connection was rejected TOE logs showing that the TLS connection was not successful.

	• Create a certificate containing a wildcard that is not in the left-most label of the presented identifier as DNS-ID Screenshot showing certificate containing a wildcard that is not in the left-most label of the presented identifier as DNS-ID. • Start TLS server with certificate containing a wildcard that is not in the left-most label of the presented identifier Screenshot of the evaluator configuring TLS server to use the invalid cert. • Attempt the connection from TOE to the TLS server using reference identifier Screenshot of the TOE initiating a TLS connection to the server. • Verify with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful. • Verify with log that connection was rejected TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The evaluator verified that the connection failed when the TLS server presented the certificate containing a wildcard that was not in the left-most label of the presented identifier. The TOE meets the test requirements.

6.4.16 FCS_TLSC_EXT.1.2 Test #5 (2)(a)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with a single left-most label (e.g. foo.example.com) and verify that the connection succeeds, if wildcards are supported, or fails if wildcards are not supported. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps & Expected Test Results	• Create a server certificate containing a wildcard in the left-most label of the presented identifier as CN-ID with DNS Screenshot showing certificate with wildcard in the left-most label of the presented identifier as CN-ID with DNS • Start TLS server with certificate containing a wildcard in the left-most label Screenshot of the evaluator configuring TLS server to use the cert • Attempt the connection from TOE to the TLS server using reference identifier with a single left-most label Screenshot of the TOE initiating a TLS connection to the server. • Verified with Wireshark that connection was successful A packet capture showing that the TLS connection was successful.

	• Verified with logs that connection was successful TOE logs showing that the TLS connection was successful. • Create a server certificate containing a wildcard in the left-most label of the presented identifier as DNS-ID Screenshot showing certificate with wildcard in the left-most label of the presented identifier as DNS-ID • Start TLS server with certificate containing a wildcard in the left-most label Screenshot of the evaluator configuring TLS server to use the cert • Attempt the connection from TOE to the TLS server using reference identifier with a single left-most label Screenshot of the TOE initiating a TLS connection to the server. • Verified with Wireshark that connection was successful A packet capture showing that the TLS connection was successful. • Verified with logs that connection was successful TOE logs showing that the TLS connection was successful.
Pass/Fail with Explanation	Pass. The connection was successful when the evaluator presented a server certificate containing a wildcard in the left-most label. The TOE meets the test requirements.

6.4.17 FCS_TLSC_EXT.1.2 Test #5 (2)(b)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier without a left-most label as in the certificate (e.g. example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps & Expected Test Results	• Create a server certificate containing a wildcard in the left-most label of the presented identifier as CN-ID with DNS Screenshot showing certificate with wildcard in the left-most label of the presented identifier as CN-ID with DNS • Start the TLS server with certificate containing a wildcard in the left-most label Screenshot of the evaluator configuring TLS server to use the valid cert • Attempt the connection from TOE to the TLS server using reference identifier without a left-most label as in the certificate Screenshot of the TOE initiating a TLS connection to the server. • Verified with Wireshark that connection failed A packet capture showing that the TLS connection was not successful.

	• Verify connection failed via log TOE logs showing that the TLS connection was not successful. • Create a server certificate containing a wildcard in the left-most label of the presented identifier as DNS-ID Screenshot showing certificate with wildcard in the left-most label of the presented identifier as DNS-ID • Start the TLS server with certificate containing a wildcard in the left-most label Screenshot of the evaluator configuring TLS server to use the valid cert • Attempt the connection from TOE to the TLS server using reference identifier without a left-most label as in the certificate Screenshot of the TOE initiating a TLS connection to the server. • Verified with Wireshark that connection failed A packet capture showing that the TLS connection was not successful. • Verify connection failed via log TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The connection failed when the evaluator presented a server certificate containing a wildcard in the left-most label and configured the reference identifier without a left-most label. The TOE meets the test requirements.

6.4.18 FCS_TLSC_EXT.1.2 Test #5 (2)(c)

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT.** Test 5: The evaluator shall perform the following wildcard tests with each supported type of reference identifier that includes a DNS name (i.e. CN-ID with DNS, DNS-ID, SRV-ID, URI-ID): The evaluator shall present a server certificate containing a wildcard in the left-most label (e.g. *.example.com). The evaluator shall configure the reference identifier with two left-most labels (e.g. bar.foo.example.com) and verify that the connection fails. (Remark: Support for wildcards was always intended to be optional. It is sufficient to state that the TOE does not support wildcards and observe rejected connection attempts to satisfy corresponding assurance activities.)
Test Steps & Expected Test Results	• Create a server certificate containing a wildcard in the left-most label of the presented identifier as CN-ID with DNS Screenshot showing certificate with wildcard in the left-most label of the presented identifier as CN-ID with DNS • Start the TLS server with certificate containing a wildcard in the left-most label Screenshot of the evaluator configuring TLS server to use the cert containing a wildcard in the left-most label • Attempt the connection from TOE to the TLS server using reference identifier with two left-most labels Screenshot of the TOE initiating a TLS connection to the server.

	• Verified with Wireshark that connection failed A packet capture showing that the TLS connection was not successful. • Verify connection failed via log TOE logs showing that the TLS connection was not successful. • Create a server certificate containing a wildcard in the left-most label of the presented identifier as DNS-ID Screenshot showing certificate with wildcard in the left-most label of the presented identifier as DNS-ID • Start the TLS server with certificate containing a wildcard in the left-most label Screenshot of the evaluator configuring TLS server to use the cert containing a wildcard in the left-most label • Attempt the connection from TOE to the TLS server using reference identifier with two left-most labels Screenshot of the TOE initiating a TLS connection to the server. • Verified with Wireshark that connection failed A packet capture showing that the TLS connection was not successful. • Verify connection failed via log TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The connection failed when the evaluator presented a server certificate containing a wildcard in the left-most label and configured the reference identifier with two left-most labels. The TOE meets the test requirements.

6.4.19 FCS_TLSC_EXT.1.2 Test #6

Item	Data
Test Assurance Activity	This test is applicable if **TLS-based communications with RFC 6125 is selected for FTP_ITC.1, FTP_TRP, or FPT_ITT**. If IP addresses are supported, the evaluator shall present a server certificate that contains a CN that matches the reference identifier, except one of the groups has been replaced with an asterisk (*) (e.g. CN=192.168.1.* when connecting to 192.168.1.20, CN=2001:0DB8:0000:0000:0008:0800:200C:* when connecting to 2001:0DB8:0000:0000:0008:0800:200C:417A). The certificate shall not contain the SAN extension. The evaluator shall verify that the connection fails. The evaluator shall repeat this test for each supported IP address version (e.g. IPv4, IPv6). Remark: Some systems might require the presence of the SAN extension. In this case the connection would still fail but for the reason of the missing SAN extension instead of the mismatch of CN and reference identifier. Both reasons are acceptable to pass Test 6.
Test Steps & Expected Test Results	Part 1 - IPv4 • Create a certificate with incorrect CN and missing SAN Screenshot showing certificate with incorrect CN and missing SAN • Start the TLS server with certificate which has incorrect CN and missing SAN Screenshot of the evaluator configuring TLS server to use the cert with incorrect CN and missing SAN

	• Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was rejected TOE logs showing that the TLS connection was not successful. • Verified with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful. Part 2 – IPv6 • Create a certificate with incorrect CN and missing SAN Screenshot showing certificate with incorrect CN and missing SAN • Start the TLS server with certificate which has incorrect CN and missing SAN Screenshot of the evaluator configuring TLS server to use the cert with incorrect CN and missing SAN • Attempt the connection from TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verified with log that connection was rejected TOE logs showing that the TLS connection was not successful. • Verified with Wireshark that connection was rejected A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The evaluator has presented a server certificate that contains a CN that matches the reference identifier where one of the groups in IP address has been replaced with an asterisk (*) and missing the SAN extension and verified that the connection failed. The TOE meets the test requirements.

6.4.20 FCS_TLSC_EXT.1.3 Test #1

Item	Data
Test Assurance Activity	Using the administrative guidance, the evaluator shall load a CA certificate or certificates needed to validate the presented certificate used to authenticate an external entity and demonstrate that the function succeeds, and a trusted channel can be established.
Test Steps & Expected Test Results	Pass. This test is covered as a part of FIA_X509_EXT.1.1 Test #1.
Pass/Fail with Explanation	Pass. This test is covered as a part of FIA_X509_EXT.1.1 Test #1.

6.4.21 FCS_TLSC_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	The evaluator shall then change the presented certificate(s) so that validation fails and show that the certificate is not automatically accepted. The evaluator shall repeat this test to cover the selected types of failure defined in the SFR (i.e. the selected ones from failed matching of the reference identifier, failed validation of the certificate path, failed validation of the expiration date, failed determination of the revocation status). The evaluator performs the action indicated in the SFR selection observing the TSF resulting in the expected state for the trusted channel (e.g. trusted channel was established) covering the types of failure for which an override mechanism is defined.

Test Steps & Expected Test Results	This test case is covered by the FIA_X509_EXT.1 test cases. The TOE does not implement any override mechanism.
Pass/Fail with Explanation	Pass. This test case is covered by the FIA_X509_EXT.1 test cases. The TOE does not implement any override mechanism.

6.4.22 FCS_TLSC_EXT.1.3 Test #3

Item	Data
Test Assurance Activity	The purpose of this test to verify that only selected certificate validation failures could be administratively overridden. **If any override mechanism is defined for failed certificate validation**, the evaluator shall configure a new presented certificate that does not contain a valid entry in one of the mandatory fields or parameters (e.g. inappropriate value in extendedKeyUsage field) but is otherwise valid and signed by a trusted CA. The evaluator shall confirm that the certificate validation fails (i.e. certificate is rejected), and there is no administrative override available to accept such certificate.
Test Steps & Expected Test Results	This test case is covered by the FIA_X509_EXT.1 test cases. Each of these test case shows an individual validation failure which is asked for by the test case. Additionally, the TOE does not implement any override mechanism
Pass/Fail with Explanation	Pass. This test case is covered by the FIA_X509_EXT.1 test cases. Each of these test case shows an individual validation failure which is asked for by the test case. Additionally, the TOE does not implement any override mechanism

6.4.23 FCS_TLSC_EXT.2.1

These tests are covered by FCS_TLSC_EXT.1 and FIA_X509_EXT.1 testing.

6.5 Update

6.5.1 FPT_TST_EXT.1 Test #1

Item	Data
Test Assurance Activity	It is expected that at least the following tests are performed: a) Verification of the integrity of the firmware and executable software of the TOE b) Verification of the correct operation of the cryptographic functions necessary to fulfil any of the SFRs. The evaluator shall either verify that the self-tests described above are carried out during initial start-up or that the developer has justified any deviation from this. For distributed TOEs, the evaluator shall perform testing of self-tests on all TOE components according to the description in the TSS about which self-test are performed by which component.
Test Steps & Expected Test Results	• Power on the TOE CLI output on the TOE being powered on. • Observe the output of the TOE start-up and ensure that evidence of the execution of self-tests are provided CLI output on the TOE performing a typical reboot and cryptographic self tests passing.

Pass/Fail with Explanation	Pass. The TOE performed claimed self-tests. The TOE meets the test requirements.

6.5.2 FPT_TUD_EXT.1 Test #1

Item	Data
Test Assurance Activity	The evaluator performs the version verification activity to determine the current version of the product as well as the most recently installed version (should be the same version before updating). The evaluator obtains a legitimate update using procedures described in the guidance documentation and verifies that it is successfully installed on the TOE. (For some TOEs loading the update onto the TOE and activation of the update are separate steps ('activation' could be performed e.g., by a distinct activation step or by rebooting the device). In that case the evaluator verifies after loading the update onto the TOE but before activation of the update that the current version of the product did not change but the most recently installed version has changed to the new product version.) After the update, the evaluator performs the version verification activity again to verify the version correctly corresponds to that of the update and that current version of the product and most recently installed version match again.
Test Steps & Expected Test Results	• Verify the current version of the TOE Screenshot showing the currently installed version of the TOE. • Perform the image update TOE command line output of the evaluator running the commands to perform an update. • Verify the new version of the TOE Screenshot showing the new version of the TOE. • Verify that a log was created reflecting the initiation of software update TOE logs showing the initiation of software update. • Verify that a log was created reflecting the successful of software update TOE logs showing that the update was successful.
Pass/Fail with Explanation	Pass. The TOE passed the image integrity test, and the software image was successfully updated. The TOE meets the test requirements.

6.5.3 FPT_TUD_EXT.1 Test #3 (a)

Item	Data
Test Assurance Activity	[conditional]: If **the TOE itself verifies a hash value over an image against a published hash value (i.e., reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE**, the following test shall be performed (otherwise the test shall be omitted). If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test.

	The evaluator obtains or produces an illegitimate update such that the hash of the update does not match the published hash. The evaluator provides the published hash value to the TOE and calculates the hash of the update either on the TOE itself (if that functionality is provided by the TOE), or else outside the TOE. The evaluator confirms that the hash values are different, and attempts to install the update on the TOE, verifying that this fails because of the difference in hash values (and that the failure is logged). Depending on the implementation of the TOE, the TOE might not allow the Security Administrator to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE If the TOE allows delayed activation of updates, the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs. Depending on the point in time when the attempted update is rejected, the most recently installed version might or might not be updated. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version, and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps & Expected Test Results	• Verify the current version of the TOE Screenshot showing the currently installed version of the TOE. • Edit the hash value in SHA-256.txt file Screenshot showing the hash value being edited. • Reboot and observe the console output that TOE failed to load the image TOE command line showing that the image failed to load.
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE rejected an update when the hash value did not match as to the published hash of the image. The TOE meets the test requirements.

6.5.4 FPT_TUD_EXT.1 Test #3 (b)

Item	Data
Test Assurance Activity	[conditional]: If **the TOE itself verifies a hash value over an image against a published hash value (i.e., reference value) that has been imported to the TOE from outside such that the TOE itself authorizes the installation of an image to update the TOE**, the following test shall be performed (otherwise the test shall be omitted). If the published hash is provided to the TOE by the Security Administrator and the verification of the hash value over the update file(s) against the published hash is performed by the TOE, then the evaluator shall perform the following tests. The evaluator first confirms that no update is pending and then performs the version verification activity to determine the current version of the product, verifying that it is different from the version claimed in the update(s) to be used in this test. The evaluator uses a legitimate update and tries to perform verification of the hash value without providing the published hash value to the TOE. The evaluator confirms that this attempt fails. Depending on the implementation of the TOE it might not be possible to attempt the verification of the hash value without providing a hash value to the TOE, e.g., if the hash value needs to be handed over to the TOE as a parameter in a command line

	message and the syntax check of the command prevents the execution of the command without providing a hash value. In that case the mechanism that prevents the execution of this check shall be tested accordingly, e.g., that the syntax check rejects the command without providing a hash value, and the rejection of the attempt is regarded as sufficient verification of the correct behaviour of the TOE in failing to verify the hash. The evaluator then attempts to install the update on the TOE (in spite of the unsuccessful hash verification) and confirms that this fails. Depending on the implementation of the TOE, the TOE might not allow to even attempt updating the TOE after the verification of the hash value fails. In that case the verification that the hash comparison fails is regarded as sufficient verification of the correct behaviour of the TOE If the TOE allows delayed activation of updates, the TOE must be able to display both the currently executing version and most recently installed version. The handling of version information of the most recently installed version might differ between different TOEs. Depending on the point in time when the attempted update is rejected, the most recently installed version might or might not be updated. The evaluator shall verify that the TOE handles the most recently installed version information for that case as described in the guidance documentation. After the TOE has rejected the update the evaluator shall verify, that both, current version, and most recently installed version, reflect the same version information as prior to the update attempt.
Test Steps & Expected Test Results	• Verify the current version of the TOE Screenshot showing the currently installed version of the TOE. • Remove the hash file from the TOE Screenshot showing the deletion of the hash file. • Reboot the TOE Screenshot showing the rebooting the TOE. • Observe console output and verify that TOE rejected to load the image TOE command line showing that the image failed to load.
Pass/Fail with Explanation	Pass. The evaluator verified that the TOE refused to accept the update when the hash file had been removed. The TOE meets the test requirements.

6.6 X509-Rev

6.6.1 FIA_X509_EXT.1.1/Rev Test #1a

Item	Data
Test Assurance Activity	Test 1a: The evaluator shall present the TOE with a valid chain of certificates (terminating in a trusted CA certificate) as needed to validate the leaf certificate to be used in the function and shall use this chain to demonstrate that the function succeeds. Test 1a shall be designed in a way that the chain can be 'broken' in Test 1b by either being able to remove the trust anchor from the TOEs trust store, or by setting up the trust store in a way that at least one intermediate CA certificate needs to be provided, together with the leaf certificate from outside the TOE, to complete the chain (e.g. by storing only the root CA certificate in the trust store).
Test Steps & Expected Test Results	• Upload a full certificate chain to the TOE for a TLS server the TOE will connect to Screenshot showing full certificate chain being uploaded to the TOE. • Verify that a log was generated when uploading the certificate change

	TOE logs showing that the upload was successful. • Attempt a TLS connection from the TOE to the configured remote TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection is established using packet capture A packet capture showing that the TLS connection was successful. • Verify the connection is established using logs TOE logs showing that the TLS connection was successful.
Pass/Fail with Explanation	Pass. The TOE connected to the TLS server with uploaded certificates. The TOE meets the test requirements.

6.6.2 FIA_X509_EXT.1.1/Rev Test #1b

Item	Data
Test Assurance Activity	Test 1b: The evaluator shall then 'break' the chain used in Test 1a by either removing the trust anchor in the TOE's trust store used to terminate the chain, or by removing one of the intermediate CA certificates (provided together with the leaf certificate in Test 1a) to complete the chain. The evaluator shall show that an attempt to validate this broken chain fails.
Test Steps & Expected Test Results	• Begin with Test 1a • Remove one of the certificates from the uploaded certificate chain and evaluator has removed an intermediary certificate named "ICA" Screenshot showing removal of ICA certificate on the TOE. • Attempt to connect from the TOE to TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify that the connection fails using packet capture A packet capture showing that the TLS connection was not successful. • Verify that the connection fails using log TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The attempt to validate certificate chain failed and the TOE rejected the connection. The TOE meets the test requirements.

6.6.3 FIA_X509_EXT.1.1/Rev Test #2

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 2: The evaluator shall demonstrate that validating an expired certificate results in the function failing.
Test Steps & Expected Test Results	• Create a certificate for a TLS server with a very short lifetime which is expired Screenshot showing an expired certificate being used by the TLS server. • Attempt a TLS connection from the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Start the TLS server

	Screenshot of the TLS server running on a remote machine • Verify the connection is refused using packet capture TOE logs showing that the TLS connection was not successful. • Verify the connection is refused using logs A packet capture showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. When an expired certificate was represented, the verification failed, and the TOE rejected the connection. The TOE meets the test requirements.

6.6.4 FIA_X509_EXT.1.1/Rev Test #3

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 3: The evaluator shall test that the TOE can properly handle revoked certificates-–conditional on whether CRL or OCSP is selected; if both are selected, then a test shall be performed for each method. The evaluator shall test revocation of the peer certificate and revocation of the peer intermediate CA certificate i.e., the intermediate CA certificate should be revoked by the root CA. The evaluator shall ensure that a valid certificate is used, and that the validation function succeeds. The evaluator then attempts the test with a certificate that has been revoked (for each method chosen in the selection) to ensure when the certificate is no longer valid that the validation function fails. Revocation checking is only applied to certificates that are not designated as trust anchors. Therefore, the revoked certificate(s) used for testing shall not be a trust anchor.
Test Steps & Expected Test Results	Part 1 • Attempt a TLS connection from the TOE to the configured remote TLS server Screenshot of the TOE initiating a TLS connection to the server. • Start the TLS server Screenshot of the TLS server running on a remote machine. • Verify the connection is established using packet capture A packet capture showing that the TLS connection was successful. • Verify the connection using logs TOE logs showing that the TLS connection was successful. Part 2 • Revoke an intermediate certificate in the uploaded certificate chain Screenshot showing revocation of ICA certificate. • Start the TLS server Screenshot of the TLS server running on a remote machine. • Attempt a TLS connection from the TOE to the configured remote TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection is not established using packet capture A packet capture showing that the TLS connection was not successful. • Verify the connection is refused using logs TOE logs showing that the TLS connection was not successful.

	• Unrevoke the intermediate certificate Screenshot showing valid ICA certificate. Part 3 • Revoke the leaf certificate of the TLS server to which the TOE will be connecting Screenshot showing revocation of leaf certificate of the TLS server. • Attempt a TLS connection from the TOE to the configured remote TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection is not established using packet capture A packet capture showing that the TLS connection was not successful. • Verify the connection is refused using log TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The TOE successfully connected to the server with a valid certificate and did not connect to the server with a revoked certificate. The TOE meets the test requirements.

6.6.5 FIA_X509_EXT.1.1/Rev Test #4

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. If OCSP is selected, the evaluator shall configure the OCSP server or use a man-in-the-middle tool to present a certificate that does not have the OCSP signing purpose and verify that validation of the OCSP response fails. If CRL is selected, the evaluator shall configure the CA to sign a CRL with a certificate that does not have the cRLsign key usage bit set and verify that validation of the CRL fails.
Test Steps & Expected Test Results	• Create a CRL that is signed by a certificate that does not have the CRLsign key usage bit set Screenshot showing a CRL signed by a certificate that does not have the CRLsign key usage bit set. • Upload to the TOE a full certificate chain for a TLS server the TOE will connect to Ensure the certificates in the chain are configured for checking using a CRL signed by the certificate that does not have the cRLsign key usage bit set Screenshot showing full certificate chain being uploaded to the TOE. • Shutdown and no shut the CA profile Screenshot showing the status of the CA profile. • Attempt to connect to the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify that the TOE gets the CRL using log Screenshot of the TOE showing the CRL update on the TOE. • Verify that the TOE rejected the connection using logs TOE logs showing that the TLS connection was not successful. • Verify that the TOE rejected the connection using packet capture A packet capture showing that the TLS connection was not successful.

Pass/Fail with Explanation	Pass. The evaluator configured the CA to sign a CRL with a certificate that does not have the CRL sign key usage set and verified that the validation of the CRL fails. The TOE meets the test requirements.

6.6.6 FIA_X509_EXT.1.1/Rev Test #5

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the first eight bytes of the certificate and demonstrate that the certificate fails to validate. (The certificate will fail to parse correctly.)
Test Steps & Expected Test Results	• Start **Acumen-TLSC** tool configured to modify a byte in the first eight bytes of the certificate Screenshot showing Acumen-TLSC tool modifying a byte in the first eight bytes of the certificate. • Attempt to establish a TLS connection from the TOE to **Acumen-TLSC** tool Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection is refused using packet capture due to the modification A packet capture showing that the TLS connection was not successful. • Verify the connection is refused using logs due to the modification TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. Modifying byte in the first eight bytes of the certificate demonstrated that the certificate failed to validate, and the TOE rejected the connection. The TOE meets the test requirements.

6.6.7 FIA_X509_EXT.1.1/Rev Test #6

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. The evaluator shall modify any byte in the certificate signatureValue field (see RFC5280 Sec. 4.1.1.3), which is normally the last field in the certificate, and demonstrate that the certificate fails to validate. (The signature on the certificate will not validate.)
Test Steps & Expected Test Results	• Start **Acumen-TLSC** tool configured to modify a byte in the certificate signatureValue field Screenshot showing Acumen-TLSC tool modifying a byte in the certificate signatureValue field. • Attempt to establish a TLS connection from the TOE to **Acumen-TLSC** tool Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection is refused using packet capture due to the modification A packet capture showing that the TLS connection was not successful. • Verify the connection is refused using logs due to the modification

	TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. Modifying a byte in the certificate signatureValue field demonstrated that the certificate failed to validate, and the TOE rejected the connection. The TOE meets the test requirements.

6.6.8 FIA_X509_EXT.1.1/Rev Test #7

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that checking the validity of a certificate is performed when a certificate is used in an authentication step or when performing trusted updates (if FPT_TUD_EXT.2 is selected). It is not sufficient to verify the status of a X.509 certificate only when it is loaded onto the TOE. Test 7: The evaluator shall modify any byte in the public key of the certificate and demonstrate that the certificate fails to validate. (The hash of the certificate will not validate.)
Test Steps & Expected Test Results	• Start **Acumen-TLSC** tool configured to modify a byte in the public key of the certificate Screenshot showing Acumen-TLSC tool modifying a byte in the public key of the certificate. • Attempt to establish a TLS connection from the TOE to **Acumen-TLSC** tool Screenshot of the TOE initiating a TLS connection to the server. • Verify the connection is refused using packet capture due to the modification A packet capture showing that the TLS connection was not successful. • Verify the connection is refused using logs due to the modification TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. Modifying any byte in the public key of the certificate demonstrated that the certificate failed to validate, and the TOE rejected the connection. The TOE meets the test requirements.

6.6.9 FIA_X509_EXT.1.2/Rev Test #1

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trustingly satisfied) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests is to verify that the TOE accepts a certificate as a CA certificate only if it has been marked as a CA certificate by using basicConstraints with the CA flag set to True (and implicitly tests that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate.

	The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 1: The evaluator shall ensure that at least one of the CAs in the chain does not contain the basicConstraints extension. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: *(i) as part of the validation of the leaf certificate belonging to this chain.* *(ii) when attempting to add a CA certificate without the basicConstraints extension to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).*
Test Steps & Expected Test Results	• Create a certificate chain for a TLS server where an intermediate CA is missing the BasicConstraints extension Screenshot showing full certificate chain where an intermediate CA is missing the BasicConstraints extension. • Attempt to upload an intermediate CA certificate to the TOE Screenshot showing ICA certificate being uploaded to the TOE. • Attempt to add an intermediate CA certificate without *basicConstraints* extension to the TOE's trust store Screenshot showing ICA certificate without *basicConstraints* extension to the TOE's trust store • Verify that the TOE rejects the certificate chain using log TOE logs showing the rejected certificate upload.
Pass/Fail with Explanation	Pass. When an intermediate certificate without the basicConstraints extension was added to the TOE's trust store, the TOE rejected the certificate. The TOE meets the test requirements.

6.6.10 FIA_X509_EXT.1.2/Rev Test #2

Item	Data
Test Assurance Activity	The tests described must be performed in conjunction with the other certificate services assurance activities, including the functions in FIA_X509_EXT.2.1/Rev. The tests for the extendedKeyUsage rules are performed in conjunction with the uses that require those rules. Where the TSS identifies any of the rules for extendedKeyUsage fields (in FIA_X509_EXT.1.1) that are not supported by the TOE (i.e. where the ST is therefore claiming that they are trustingly satisfied) then the associated extendedKeyUsage rule testing may be omitted. The goal of the following tests it to verify that the TOE accepts only certificates that have been marked as CA certificates by using basicConstraints with the CA flag set to True (and implicitly that the TOE correctly parses the basicConstraints extension as part of X509v3 certificate chain validation). For each of the following tests the evaluator shall create a chain of at least three certificates: - a self-signed root CA certificate, - an intermediate CA certificate and - a leaf (node) certificate.

	The properties of the certificates in the chain are adjusted as described in each individual test below (and this modification shall be the only invalid aspect of the relevant certificate chain). Test 2: The evaluator shall ensure that at least one of the CA certificates in the chain has a basicConstraints extension in which the CA flag is set to FALSE. The evaluator confirms that the TOE rejects such a certificate at one (or both) of the following points: i. As part of the validation of the leaf certificate belonging to this chain. ii. When attempting to add a CA certificate with the CA flag set to FALSE to the TOE's trust store (i.e. when attempting to install the CA certificate as one which will be retrieved from the TOE itself when validating future certificate chains).
Test Steps & Expected Test Results	• Create a certificate chain for a TLS server where an intermediate CA has the *basicConstraints* extension configured to false Screenshot showing ICA certificate with the BasicConstraints extension configured to false. • Attempt to upload the certificate chain to the TOE Screenshot showing ICA certificate being uploaded to the TOE. • Attempt to add an intermediate CA certificate configured *basicConstraints* extension FALSE to the TOE's trust store Screenshot showing ICA certificate with *basicConstraints* extension configured to false being updated to the TOE's trust store. • Verify that the TOE rejects the certificate using log TOE logs showing the rejected certificate upload.
Pass/Fail with Explanation	Pass. The TOE rejected an intermediate CA with the Basic Constraints which was set to FALSE. The TOE meets the test requirements.

6.6.11 FIA_X509_EXT.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall perform the following test for each trusted channel: The evaluator shall demonstrate that using a valid certificate that requires certificate validation checking to be performed in at least some part by communicating with a non-TOE IT entity. The evaluator shall then manipulate the environment so that the TOE is unable to verify the validity of the certificate and observe that the action selected in FIA_X509_EXT.2.2 is performed. If the selected action is administrator-configurable, then the evaluator shall follow the guidance documentation to determine that all supported administrator-configurable options behave in their documented manner.
Test Steps & Expected Test Results	• Start the TLS server Screenshot of the TLS server running on a remote machine. • Connect the TOE to the TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify the successful connection using Wireshark A packet capture showing that the TLS connection was successful. • Verify the successful connection using logs TOE logs showing that the TLS connection was successful. • Make the CRL distribution point unavailable

	Screenshot showing CRL distribution point being unavailable. • Remove ICA.crl file from local system-pki directory TOE logs showing ICA.crl being removed from the local system-pki. • To verify that the TOE reaches to CRL server to fetch the CRL file execute the "shutdown" and "no shutdown" command at ICA profile TOE command line shows the successful exection of the commands. • Start the TLS server Screenshot of the TLS server running on a remote machine. • Attempt a TLS connection from the TOE to the configured remote TLS server Screenshot of the TOE initiating a TLS connection to the server. • Verify that the connection is not successful using packet capture A packet capture showing that the TLS connection was not successful. • Verify that the connection is not successful using log TOE logs showing that the TLS connection was not successful.
Pass/Fail with Explanation	Pass. The evaluator manipulated the environment so that the TOE was unable to verify the validity of the certificate, and the TOE rejected the connection. The TOE meets the test requirements.

6.6.12 FIA_X509_EXT.3 Test #1

Item	Data
Test Assurance Activity	The evaluator shall use the guidance documentation to cause the TOE to generate a Certification Request. The evaluator shall capture the generated message and ensure that it conforms to the format specified. The evaluator shall confirm that the Certification Request provides the public key and other required information, including any necessary user-input information.
Test Steps & Expected Test Results	• From the TOE generate a CSR TOE logs showing the generation of a CSR. • Open the CSR to review the contents and verify the Public key, Common Name, Organization, Organizational Unit and Country Screenshot of the TLS server showing the details of CSR.
Pass/Fail with Explanation	Pass. The evaluator confirmed that the CSR provided the public key and other required information. The TOE meets the test requirements.

6.6.13 FIA_X509_EXT.3 Test #2

Item	Data
Test Assurance Activity	The evaluator shall demonstrate that validating a response message to a Certification Request without a valid certification path results in the function failing. The evaluator shall then load a certificate or certificates as trusted CAs needed to validate the certificate response message and demonstrate that the function succeeds.
Test Steps & Expected Test Results	Part 1 • From the TOE, generate a CSR TOE logs showing the generation of a CSR. • Generate a signed certificate based on the generated CSR from an external CA Screenshot of the CSR signed by an external CA.

	• Remove an intermediate certificate using the notepad++ editor from the chain of certificates Screenshot of the editor without the intermediate certificate • Attempt to load the signed certificate to the TOE Screenshot showing the modified certificate being loaded into the TOE. • Verify that the TOE rejects the certificate because the full trust chain of the CA is not present using log TOE logs showing that the certificate upload was not successful. Part 2 • Modify the chain of certificates and add an intermediate certificate which was removed in part 1 Screenshot of the editor after adding the intermediate certificate. • Re-attempt to load the signed certificate on the TOE Screenshot showing the modified certificate being loaded into the TOE. • Verify that the TOE accepts the certificate using log TOE logs showing that the certificate upload was successful.
Pass/Fail with Explanation	Pass. CSR responses signed by a CA without a full trust path were not installed on the TOE. The TOE installed a CSR response signed by a CA with a full trust path. The TOE meets the test requirements.

6.7 MACsec

6.7.1 FAU_GEN.1/MACSEC Test #1

Item	Data
Test Assurance Activity	The evaluator shall complete the assurance activity for FAU_GEN.1 as described in the NDcPP for the auditable events defined above in addition to the applicable auditable events that are defined in the NDcPP. The evaluator shall also ensure that the administrative actions defined for this EP are appropriately audited.
Test Steps & Expected Test Results	NOTE: This test case is covered by collecting audit records from each applicable test case • In each test case, collect the audit records required by the Extended Package **The TOE is able to generate audit records for all auditable events required by the Extended Package.**
Pass/Fail with Explanation	Pass. The TOE generated the required audit records which were collected after the execution of applicable test cases. The TOE meets the test requirements.

6.7.2 FCS_MACSEC_EXT.1 Test #1

Item	Data

Test Assurance Activity	The evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the Operational Environment and verify that the TSF logs the communications. The evaluator shall capture the traffic between the TOE and the Operational Environment to determine the SCI that the TOE uses to identify the peer. The evaluator shall then configure a test system to capture traffic between the peer and the TOE to modify the SCI that is used to identify the peer. The evaluator then verifies that the TOE does not reply to this traffic and logs that the traffic was discarded.
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify that the TOE logs configuration of the service TOE logs showing the creation and activation of macsec configuration. • Start connection Screenshot of the TOE initiaing a macsec connection with the peer. • Verify the MACsec connection is established using logs TOE logs showing that the MACsec connection was successful. • Verify the SCI used between the TOE and the peer using packet capture A packet capture showing the original SCI used between the TOE and the peer. • Modify the SCI from the peer (this is done using Acumen-MACsec tool) Screenshot of the Acumen MACsec modifying the SCI. • Verify the TOE rejects modified traffic by packet capture A packet capture showing the modified traffic being rejected. • Verify the TOE rejects modified traffic by log TOE logs showing the modified traffic being rejected

Pass/Fail with Explanation	Pass. The MACsec connection was established successfully. During the modsci test, modified SCI packets were rejected by the TOE. The TOE meets the test requirements.

6.7.3 FCS_MACSEC_EXT.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall send Ethernet traffic to the TOE's MAC address that iterates through the full range of supported EtherType values (refer to http://standards.ieee.org/develop/regauth/ethertype/eth.txt) and observes that traffic for all EtherType values is discarded by the TOE except for the traffic which has an EtherType value of 88-8E, 88-E5 or 8808. Note that there are large number of EtherType values, so the evaluator is encouraged to execute a script that automatically iterates through each value. ***TD0553 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify that the TOE logs configuration of the service TOE logs showing the creation and activation of macsec configuration. • Start connection Screenshot of the TOE initiating a macsec connection with the peer. • Verify the MACsec connection is established TOE logs showing that the MACsec connection was successful.

	• Send Ethernet traffic to the TOE's MAC address that iterates through the full range of supported EtherType values (this is done using Acumen-MACsec tool) Screenshot of the Acumen MACsec sending traffic iterating full range of supported EtherType values. • Verify that TOE does not respond to any EtherType other than 88-8E and 88-E5 using packet capture TOE logs showing that the TOE accepts only EtherType value of 88-8E, 88-E5 or 8808.
Pass/Fail with Explanation	Pass. Ether type other than 88-8E and 88-E5 were rejected by the TOE. The TOE meets the test requirements.

6.7.4 FCS_MACSEC_EXT.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall transmit MACsec traffic to the TOE from a MACsec-capable peer in the Operational Environment. The evaluator shall verify using packet captures and/or audit logs that the frame bytes after the MACsec Tag values in the received traffic is not obviously predictable.
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify that the TOE logs configuration of the service TOE logs showing the creation and activation of macsec configuration. • Transmit MACsec traffic to the TOE from the peer

	Screenshot of the TOE initiaing a macsec connection with the peer. • Verify the MACsec connection is established TOE logs showing that the MACsec connection was successful. • Verify using packet capture that the frame bytes after the MACsec Tag values in the received traffic is not obviously predictable. A packet capture showing that MACsec traffic is not predictable.
Pass/Fail with Explanation	Pass. The MACsec packets that were transmitted between the TOE and the peer were not obviously predictable. The TOE meets the test requirements.

6.7.5 FCS_MACSEC_EXT.2 Test #2

Item	Data
Test Assurance Activity	The evaluator shall transmit valid MACsec traffic to the TOE from a MACsec-capable peer in the operational environment that is routed through a test system set up as a man-in-the-middle. The evaluator shall use the test system to intercept this traffic to modify one bit in a packet payload before retransmitting to the TOE. The evaluator shall verify that the traffic is discarded due to an integrity failure.
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Start connection Screenshot of the TOE initiaing a macsec connection with the peer. • Verify the MACsec connection is established

	TOE logs showing that the MACsec connection was successful. • Using a man-in-the-middle tool (Acumen-MACsec tool) modify a bit in each packet Screenshot of the Acumen MACsec tool modifying a bit in each packet. • Verify that the TOE rejects modified traffic using packet capture A packet capture showing the modified traffic being rejected.
Pass/Fail with Explanation	Pass. Modified ICV packets were rejected by the TOE due to an integrity failure. The TOE meets the test requirements.

6.7.6 FCS_MACSEC_EXT.4 Test #1

Item	Data
Test Assurance Activity	For each supported method of peer authentication in FCS_MACSEC_EXT.4.1, the evaluator shall follow the operational guidance to configure the supported method (if applicable). The evaluator shall set up a packet sniffer between the TOE and a MACsec-capable peer in the Operational Environment. The evaluator shall then initiate a connection between the TOE and the peer such that authentication occurs, and a secure connection is established. The evaluator shall wait 1 minute and then disconnect the TOE from the peer and stop the sniffer. The evaluator shall use the packet captures to verify that the secure channel was established using the selected mechanism and that the EtherType of the first data frame sent between the TOE and the peer is 88-E5.
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port.

	• Verify the MACsec connection is established TOE logs showing that the MACsec connection was successful. • Ensure that traffic between the connections can be captured A packet capture showing the MACsec successful connection. • Disconnect the TOE from the peer on the bridge for 1 minute and after 1 minutes, reestablish the MACsec connection between the peer and the TOE The brige command line showing the macsec being disconnected for 1 minute and reconnected after 1 minutes • Verify using packet capture that MACsec was reestablished and the EtherType of the first data frame sent between the TOE and the peer is 88-E5 A packet capture showing the successful MACsec reconnection and the EtherType of 88-E5.
Pass/Fail with Explanation	Pass. After the MACsec connection was reestablished, the first data frame that was sent between the TOE and the peer was of EtherType 88-E5. The TOE meets the test requirements.

6.7.7 FCS_MACSEC_EXT.4 Test #2

Item	Data
Test Assurance Activity	The evaluator shall capture traffic between the TOE and a MACsec-capable peer in the Operational Environment. The evaluator shall then cause the TOE to distribute a SAK to that peer, capture the MKPDUs from that operation, and verify the key is wrapped in the captured MKPDUs. ***TD0273 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values

	TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established TOE logs showing that the MACsec connection was successful. • Ensure that traffic between the connections can be captured A packet capture showing the MACsec successful connection. • From the TOE distribute a SAK to the peer A packet capture showing the TOE as a key server and a SAK being distributed. • Verify the key is wrapped in the captured MKPDU A packet capture showing SKA is wrapped in AES
Pass/Fail with Explanation	Pass. The keys were wrapped within the captured MKPDUs. The TOE meets the test requirements.

6.7.8 FCS_MKA_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	The evaluator shall use a peer device to send traffic to the TOE, arbitrarily inducing artificial delays in their transmission using a man-in-the-middle setup. The evaluator shall observe that traffic delayed longer than 2.0 seconds is rejected. ***TD0105 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values.

	• Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify that the TOE logs configuration of the service TOE logs showing the creation and activation of macsec configuration. • Enable the delay-protection on the TOE TOE logs showing the delay-protection being enabled. • Using the man-in-the-middle server introduce delays of 2.0 seconds and greater in traffic sent from the peer Screenshot of the Acumen MACsec tool introducing delays of 2.0 seconds. • Verify the MKA Session Statistics for port 1/1/1 before the delay was introduced TOE logs showing MKA Session Statistics for port 1/1/1 before the delay. • Verify the MKA Session Statistics for port 1/1/1 after the delay was introduced TOE logs showing MKA Session Statistics for port 1/1/1 after the delay. • Verify that the TOE rejects modified traffic using packet capture A packet capture showing the TOE rejecting the modified traffic. • Verify that the TOE's output which show the list of Live Peer TOE command line output showing the list of Live Peer.
Pass/Fail with Explanation	Pass. When the traffic was delayed longer than 2.0 seconds, the frames were rejected by TOE. The TOE meets the test requirements.

6.7.9 FCS_MKA_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator shall transmit MKA traffic (MKPDUs) to the TOE from an MKA-capable peer in the Operational Environment. The evaluator shall verify using packet captures and/or audit logs that the last 16 octets of the MKPDUs in the received traffic do not appear to be predictable.
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec

	TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify that the TOE logs configuration of the service TOE logs showing the creation and activation of macsec configuration. • Transmit MKA traffic (MKPDUs) to the TOE from the peer Screenshot showing the peer sending MKA traffic to the TOE. • Verify that the last 16 octets of the MKPDU do not appear to be predictable using packet capture A packet capture showing the MKPDU are not predictable.
Pass/Fail with Explanation	Pass. The last 16 octets of the MKPDU did not appear to be predictable. The TOE meets the test requirements.

6.7.10 FCS_MKA_EXT.1.4 Test #2

Item	Data
Test Assurance Activity	The evaluator shall transmit valid MKA traffic to the TOE from an MKA-capable peer in the operational environment that is routed through a test system set up as a man-in-the-middle. The evaluator shall use the test system to intercept this traffic to modify one bit in a packet payload before retransmitting to the TOE. The evaluator shall verify that the traffic is discarded due to an integrity failure.
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE.

	• Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify that the TOE logs configuration of the service TOE logs showing the creation and activation of macsec configuration. • Verify live peer list before sending modified byte Screenshot showing the list of Live Peer. • Modify a frame byte in transit by using the Acumen-MACsec tool Screenshot of the Acumen MACsec tool modifying a byte in transit. • Verify the traffic is modified from peer using Wireshark A packet capture showing the TOE rejecting the modified traffic. • Verify the traffic is discarded due to an integrity failure with TOE output Screenshot showing the traffic is discarded due to an integrity failure • Verify the traffic is discarded due to an integrity failure using TOE Live Peer list output Screenshot showing no active Live Peer on the TOE.
Pass/Fail with Explanation	Pass. When a modified MKPDU was detected, the traffic was discarded due to an integrity failure. The TOE meets the test requirements.

6.7.11 FCS_MKA_EXT.1.5 Test #1

Item	Data
Test Assurance Activity	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor (peer). The evaluator shall then perform the following tests using a traffic sniffer to capture this traffic. Test 1: The evaluator shall send a fresh SAK that includes both peers as active participants. The evaluator shall start an MKA session between the TOE and the two active participant peers and send MKPDUs. The evaluator shall verify from packet captures that MKPDUs are sent at least once every half-second. ***TD0105 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create

	TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established between the group TOE logs showing the successful MACsec connection. • Send a fresh SAK that includes both peers as active participants Screenshot showing the TOE as a key server and SAK being distributed. • Verify using packet capture that the MKPDUs are sent every half-second during the MKA session A packet capture showing the MKPDUs are sent every half-second.
Pass/Fail with Explanation	Pass. The MKPDUs were sent at least every half-second and visible in the packet capture. The TOE meets the test requirements.

6.7.12 FCS_MKA_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor (peer). The evaluator shall then perform the following tests using a traffic sniffer to capture this traffic. Test 2: Disconnect one of the peers. Using a man-in-the-middle device, arbitrarily introduce an artificial delay in sending a fresh SAK following the change in the Live Peer List. Repeat Test 1 delaying a fresh SAK for MKA Lifetime traffic and observe that the timeout of 6.0 seconds is enforced by the TSF. ***TD0105 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info

	TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established between the group TOE logs showing the successful MACsec connection. • Use a man-in-the-middle tool (Acumen-MACsec tool) test tool to delay the SAK for 6 seconds Screenshot of the Acumen MACsec tool delaying the SAK for 6 seconds. • Verify that the delay of the SAK for 6 seconds using packet capture A packet capture showing the delay of the SAK for 6 seconds. • Verify that the traffic was rejected using live peer list on the TOE Screenshot showing there are no active Live Peer on the TOE live peer list. • Verify that the new SAK were generated using new AN number Screenshot showing the TOE generating new SAK. • Verify that the traffic was rejected using previous AN number's statistics Screenshot showing the TOE rejected the traffic.
Pass/Fail with Explanation	Pass. The traffic delay of 6 seconds caused the MACsec connection to fail. The TOE meets the test requirements.

6.7.13 FCS_MKA_EXT.1.8 Test #1

Item	Data
Test Assurance Activity	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests: Test 1: The evaluator shall perform the following steps: 1. Load one PSK onto the TOE and device B and a second PSK onto the TOE and device C. This defines two pairwise CAs.

	2. Generate a group CAK for the group of 3 devices using ieee8021XKayCreateNewGroup. 3. Observe using packet capture that the TOE distributes the group CAK to the two peers, protected by AES key wrap using their respective PSKs. 4. Verify that B can form a SA with C and connect securely. 5. Disable the KaY functionality of device C using ieee8021XPaePortKayMkaEnable. 6. Generate a group CAK for the TOE and B using ieee8021XKayCreateNewGroup and observe they can connect. 7. The evaluator shall have B attempt to connect to C and observe this fails. 8. Re-enable the KaY functionality of device C. 9. Invoke ieee8021XKayCreateNewGroup again. 10. Verify that both the TOE can connect to C and that B can connect to C. ***TD0105 has been applied.***
Test Steps & Expected Test Results	N/A – The TOE does not generate a group CAK.
Pass/Fail with Explanation	N/A – The TOE does not generate a group CAK.

6.7.14 FCS_MKA_EXT.1.8 Test #2a

Item	Data
Test Assurance Activity	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests: Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps: 1. Send an MKPDU to the TOE's individual MAC address from a peer. Verify the frame is dropped and logged. ***TD0105 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info

	TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established between the group TOE logs showing the successful MACsec connection. • Send an MKPDU to the TOE's individual MAC address from a peer using acumen tool Screenshot of the Acumen MACsec tool sending an MKPDU to the TOE's individual MAC address. • Verify the frame is dropped using packet capture A packet capture showing the TOE rejecting the frame. • Verify the frame is dropped using TOE's output under the sub-port statistics Screenshot showing MKA Session Statistics for port 1/1/1 after the delay.
Pass/Fail with Explanation	Pass. The TOE discarded MKPDUs when they were sent from a peer to the TOE's individual MAC address. The TOE meets the test requirements.

6.7.15 FCS_MKA_EXT.1.8 Test #2b

Item	Data
Test Assurance Activity	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests: Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps: 2. Send an MKPDU to the TOE that is less than 32 octets long. Verify the frame is dropped and logged. ***TD0105 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info

	TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established between the group TOE logs showing the successful MACsec connection. • Send an MKPDU to the TOE that is less than 32 octets long. Screenshot of the Acumen MACsec tool sending an MKPDU to the TOE's individual MAC address. • Verify the frame is dropped using packet capture A packet capture showing the TOE rejecting the frame. • Verify the frame is dropped using log TOE logs showing the frame being dropped. • Verify the PDU size was small under the MKA session statistics on the TOE's output Screenshot showing MKA Session Statistics for port 1/1/1.
Pass/Fail with Explanation	Pass. When an MKPDU sent to the TOE was less than 32 octet long, it was dropped by the TOE. The "MACsec MKA operational State" changes to "out of service". The TOE meets the test requirements.

6.7.16 FCS_MKA_EXT.1.8 Test #2c

Item	Data
Test Assurance Activity	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests: Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps: 3. Send an MKPDU to the TOE whose length in octets is not a multiple of 4. Verify the frame is dropped and logged. ***TD0105 has been applied.***

Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established between the group TOE logs showing the successful MACsec connection. • Send an MKPDU to the TOE whose length in octets is not a multiple of 4. Screenshot of the Acumen MACsec tool sending an MKPDU to the TOE's individual MAC address. • Verify the frame is dropped using packet capture A packet capture showing the TOE rejecting the frame. • Verify that before 6 seconds live peer was there with packet capture and TOE's output of Peer Member Identifier A packet capture showing a live peer before 6 seconds. Screenshot showing live peer list using MKA Session Statistics for port 1/1/1. • Verify that after 6 seconds live peer was not there with packet capture and TOE's output of Peer Member Identifier A packet capture showing no live peer after 6 seconds. Screenshot showing no live peer list using MKA Session Statistics for port 1/1/1. • Verify the frame is dropped using log TOE logs showing the frame being dropped.
Pass/Fail with Explanation	Pass. When an MKPDU with the octet length, which was not in a multiple of 4, was sent to the TOE, the frames were dropped, and the session ended. The TOE meets the test requirements.

6.7.17 FCS_MKA_EXT.1.8 Test #2d

Item	Data
Test Assurance Activity	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests: Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps: 4. Send an MKPDU to the TOE that is one byte short. Verify the frame is dropped and logged. ***TD0105 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established between the group TOE logs showing the successful MACsec connection. • Send an MKPDU to the TOE that is one byte short. Screenshot of the Acumen MACsec tool sending an MKPDU that is one byte short to the TOE's individual MAC address. • Verify the frame is dropped using packet capture A packet capture showing the TOE rejecting the frame. • Verify that before 6 seconds live peer was there with packet capture and TOE's output of Peer Member Identifier A packet capture showing a live peer before 6 seconds.

	Screenshot showing live peer list using MKA Session Statistics for port 1/1/1. • Verify that after 6 seconds live peer was not there with packet capture and TOE's output of Peer Member Identifier A packet capture showing no live peer after 6 seconds. Screenshot showing no live peer list using MKA Session Statistics for port 1/1/1. • Verify the frame is dropped using log TOE logs showing the frame being dropped.
Pass/Fail with Explanation	Pass. When an MKPDU that was one byte short was sent to the TOE, the frames were dropped, and session was ended. The TOE meets the test requirements.

6.7.18 FCS_MKA_EXT.1.8 Test #2e

Item	Data
Test Assurance Activity	The tests below require the TOE to be deployed in an environment with two MACsec-capable peers, identified as devices B and C, that the TOE can communicate with. Prior to performing these tests, the evaluator shall follow the steps in the guidance documentation to configure the TOE as the Key Server and principal actor. The evaluator shall then perform the following tests: Test 2: The evaluator shall start an MKA session between the TOE and the two environmental MACsec peers and then perform the following steps: 5. Send an MKPDU to the TOE with unknown Agility Parameter. Verify the frame is dropped and logged. ***TD0105 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values

	TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established between the group TOE logs showing the successful MACsec connection. • Send an MKPDU from the TOE with unknown Agility Parameter Screenshot of the Acumen MACsec tool sending an MKPDU with unknown Agility Parameter to the TOE's individual MAC address. • Verify the frame is dropped using packet capture A packet capture showing the TOE rejecting the frame. • Verify that before 6 seconds live peer was there with packet capture and TOE's output of Peer Member Identifier A packet capture showing a live peer before 6 seconds. Screenshot showing live peer list using MKA Session Statistics for port 1/1/1. • Verify that after 6 seconds live peer was not there with packet capture and TOE's output of Peer Member Identifier A packet capture showing no live peer after 6 seconds. Screenshot showing no live peer list using MKA Session Statistics for port 1/1/1. • Verify the modified agility is logged into TOE using TOE's Output Screenshot showing MKA Session Statistics for port 1/1/1 for the logging of modified agility. • Verify the frame is dropped using log TOE logs showing the frame being dropped.
Pass/Fail with Explanation	Pass. When an MKPDU with unknown Agility Parameter was sent to the TOE, the frames were dropped, and session ended. The TOE meets the test requirements.

6.7.19 FIA_PSK_EXT.1/MACSEC Test #1

Item	Data
Test Assurance Activity	The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case. Test 1 [conditional]: If the TOE supports pre-shared keys of multiple lengths, the evaluator shall use the minimum length; the maximum length; a length inside the allowable range; and invalid lengths beyond the supported range (both higher and lower). The minimum, maximum, and included length tests should be successful, and the invalid lengths must be rejected by the TOE.
Test Steps & Expected Test Results	• Configure the TOE for PSKs that are 32 digits using command /configure macsec connectivity-association "NIAP_TOE_128_256_01" static-cak pre-shared-key 1 encryption-type aes-128-cmac create cak Screenshot of the TOE command line showing the configuration of the PSK. • Attempt to input a key that is less than 32 digits Screenshot of the TOE command line showing an attempt to input 30 digits. • Verify that the TOE rejects the PSK TOE'S Output

	Screenshot of the TOE command line rejecting the 30 digit key • Attempt to input a key that is more than 32 digits Screenshot of the TOE command line showing an attempt to input 33 digits. • Verify that the TOE rejects the PSK TOE'S Output Screenshot of the TOE command line rejecting the 33 digit key • Attempt to input a 32-digit key Screenshot of the TOE command line showing an attempt to input 32 digits. • Verify that the TOE accepts the PSK TOE'S Output Screenshot of the TOE command line accepting the 32 digit key • Configure the TOE for PSKs that are 64 digits using command /configure macsec connectivity-association "NIAP_TOE_128_256_01" static-cak pre-shared-key 2 encryption-type aes-256-cmac create cak Screenshot of the TOE command line showing configuration of the PSK. • Attempt to input a key that is less than 64 digits Screenshot of the TOE command line showing an attempt to input 63 digits. • Verify that the TOE rejects the PSK TOE'S Output Screenshot of the TOE command line rejecting the 63 digit key • Attempt to input a key that is more than 64 digits Screenshot of the TOE command line showing an attempt to input 65 digits. • Verify that the TOE rejects the PSK TOE'S Output Screenshot of the TOE command line rejecting the 65 digit key • Attempt to input a 64-digit key Screenshot of the TOE command line showing an attempt to input 64 digits. • Verify that the TOE accepts the PSK TOE'S Output Screenshot of the TOE command line accepting the 64 digit key
Pass/Fail with Explanation	Pass. The TOE only accepted defined length of pre-shared keys and rejected all the invalid keys. The TOE meets the test requirements.

6.7.20 FIA_PSK_EXT.1/MACSEC Test #2

Item	Data
Test Assurance Activity	The evaluator shall also perform the following tests for each protocol (or instantiation of a protocol, if performed by a different implementation on the TOE). Note that one or more of these tests can be performed with a single test case. Test 2 [conditional]: If the TOE does not generate bit-based pre-shared keys, the evaluator shall obtain a bit-based pre-shared key of the appropriate length and enter it according to the instructions in the operational guidance. The evaluator shall then demonstrate that a successful protocol negotiation can be performed with the key.
Test Steps & Expected Test Results	• Configure the TOE for PSKs that are 32 digits using command /configure macsec connectivity-association "NIAP_TOE_128_256_01" static-cak pre-shared-key 1 encryption-type aes-128-cmac create cak Screenshot of the TOE command line showing the configuration of the PSK. • Attempt to input a 32-digit bit-based key Screenshot of the TOE command line showing an attempt to input 32 digits. • Verify that the TOE accepts the PSK using TOE's output

	Screenshot of the TOE command line accepting the 32 digit key • Configure the TOE for PSKs that are 64 digits using command /configure macsec connectivity-association "NIAP_TOE_128_256_01" static-cak pre-shared-key 2 encryption-type aes-256-cmac create cak Screenshot of the TOE command line showing configuration of the PSK. • Attempt to input a 64-digit bit-based key Screenshot of the TOE command line showing an attempt to input 64 digits. • Verify that the TOE accepts the PSK using TOE's output Screenshot of the TOE command line accepting the 64 digit key • Show a successful MACsec negotiation with the key A packet capture showing the successful MACsec negotiation.
Pass/Fail with Explanation	Pass. The TOE accepted PSKs that were 32-digit bit-based key and 64-digit bit-based key and the TOE made successful connection with the peer. The TOE meets the test requirements.

6.7.21 FMT_SMF.1/MACSEC Test #1

Item	Data
Test Assurance Activity	Test 1: The evaluator shall connect to the PAE of the TOE and install a PSK. The evaluator shall then specify a CKN and that the PSK is to be used as a CAK. • Repeat this test for both 128-bit and 256-bit key sizes. • Repeat this test for a CKN of valid length (1-32 octets), and observe success. • Repeat this test again for CKN of invalid lengths zero and 33, and observe failure. ***TD0512 has been applied.***
Test Steps & Expected Test Results	• Configure the TOE for 128-bit CAK using command /configure macsec connectivity-association "NIAP_TOE_128_256_01" static-cak pre-shared-key 1 encryption-type aes-128-cmac create cak Screenshot of the TOE command line showing configuration of the PSK 1. • Create a CAK that is 128-bits TOE command line output of the command string that the TOE uses to create CAK values. • Verify that the CAK was created • Screenshot of the TOE command line output showing the successful creation of the CAK. • Configure the TOE for 256-bit CAKs Screenshot of the TOE command line showing configuration of the PSK 2. • Create a CAK that is 256-bits TOE command line output of the command string that the TOE uses to create CAK values. • Verify that the CAK was created • Screenshot of the TOE command line output showing the successful creation of the CAK. • Create a CKN that is between 1 and 32 octets Screenshot of the TOE command line showing an attempt to input 32 digits. • Verify that the CKN was created Screenshot of the TOE command line accepting the 32 digit key • Attempt to create a CKN that is 0 octets in length

	Screenshot of the TOE command line showing an attempt to input 0 digits. • Verify that the attempt fails Screenshot of the TOE command line rejecting the 0 digit key • Attempt to create a CKN that is 33 octets in length Screenshot of the TOE command line showing an attempt to input 33 digits. • Verify that the attempt fails Screenshot of the TOE command line rejecting the 33 digit key
Pass/Fail with Explanation	Pass. The TOE accepted the correct length of octet values for CKN. Incorrect lengths of octet values were rejected for the CKN. The TOE meets the test requirements.

6.7.22 FMT_SMF.1/MACSEC Test #2

Item	Data
Test Assurance Activity	The evaluator shall set up an environment where the TOE can connect to two other MACsec devices, identified as devices B and C, with the ability of pre-shared keys to be distributed between them. The evaluator shall configure the devices so that the TOE will be elected key server and principal actor, i.e., has highest key server priority. The evaluator will test the ability of the TOE to enable and disable MKA participants using the management function specified in the ST. The evaluator shall install pre-shared keys in devices B and C and take any necessary additional steps to create corresponding MKA participants. The evaluator shall disable the MKA participant on device C, then observe that the TOE can communicate with B but neither the TOE nor B can communicate with device C. The evaluator shall re-enable the MKA participant of device B and observe that the TOE is now able to communicate with devices B and C. ***TD0512 has been applied.***
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with two peers (same configurations are on the peer B and Peer C except IP address) TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2. • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec

	TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Ensure that IP-layer routing is set up such that the two peers can connect to each other's L3 addresses Screenshot of the Peer B making a ping connection to Peer C. • Turn off MACsec on Device B (peer 1) Screenshot of the Peer B disabling the macsec connectivity association. • Ensure that Device B can now no longer connect to Device C Screenshot of the Peer B unable to make the macsec connection with Peer C. • Re-enable the MKA participant Screenshot of the Peer B enabling the macsec connectivity association. • Verify that TOE can communicate to device B and C Screenshot of the TOE making a successful macsec connection with Peer B. A packet capture showing the successful MACsec negotiation. Screenshot of the TOE making a successful macsec connection with Peer C. A packet capture showing the successful MACsec negotiation.
Pass/Fail with Explanation	Pass. When a non-TOE peer turned off the MACsec configuration, the TOE did not accept the traffic and the two peers could not communicate with each other through the TOE. The TOE meets the test requirements.

6.7.23 FMT_SMF.1/MACSEC Test #3a

Item	Data
Test Assurance Activity	For TOEs using only PSKs, the TOE should be the Key Server in both tests and only one peer (B) needs to be tested. The tests are: Subtest a (Switch to unexpired CKN): TOE and Peer B have CKN1(10 minutes) and CKN2(20 minutes). The TOE and Peer B start using CKN1 and after 10 minutes, verify that the TOE distributes a new SAK to the peer using CKN2. ***TD0512 has been applied.***
Test Steps & Expected Test Results	• Configure the TOE MACsec key to expire in ten minutes using script (Peer has same configurations) TOE command line output showing the script and cron configuration of primary MACsec key to expire in ten minutes. • Set secondary key to expire in twenty minutes TOE command line output showing the script and cron configuration of secondary MACsec key to expire in twenty minutes. • Establish connection and allow first key to expire Screenshot showing a successful macsec connection. • Confirm that rekey occurs using CKN2 using logs. TOE logs showing rekey occured using CKN2.

	• Confirm that rekey occurs using CKN2 using packet capture A packet capture showing rekey occured using CKN2.
Pass/Fail with Explanation	Pass. The Key expired after 10 minutes and TOE distributed a new SAK to the peer using CKN2. The TOE meets the test requirements.

6.7.24 FMT_SMF.1/MACSEC Test #3b

Item	Data
Test Assurance Activity	Test 3: For TOEs using only PSKs, the TOE should be the Key Server in both tests and only one peer (B) needs to be tested. The tests are: Subtest b (reject CA with expired CKN): TOE has CKN1(10 minutes) and CKN2(20 minutes). Peer B has CKN1(20 minutes). TOE and Peer B start using CKN1 and after 10 minutes, verify that the TOE rejects (or ignores) peer's request to use (or distribute a) SAK using CKN1. ***TD0512 has been applied.***
Test Steps & Expected Test Results	• Configure the TOE MACsec key to expire in ten minutes TOE command line output showing the script and cron configuration of primary MACsec key to expire in ten minutes. • Configure the secondary key to expire in twenty minutes TOE command line output showing the script and cron configuration of secondary MACsec key to expire in twenty minutes. • Configure the first peer key to expire in twenty minutes; do not create a second key Peer B command line output of the evaluator creating only PSK 1 but not PSK 2.. • Check the time Screenshot showing the current time on the TOE. • Establish a connection and allow the first key to expire Screenshot showing a successful macsec connection with Peer B. • Confirm that rekey occurs but connection fails due to peer using old key using logs TOE logs showing rekey occured using CKN2. • Verify peer has still old CKN1 Screenshot showing Peer B still has old CKN1 • Confirm that rekey occurs but connection fails due to peer using old key using packet capture A packet capture showing rekey occured using CKN2 on the TOE, but connection fails due to peer using old key using packet capture
Pass/Fail with Explanation	Pass. The TOE rejected (or ignoreed) peer's request to use (or distribute a) SAK using CKN1. The TOE meets the test requirements.

6.7.25 FMT_SMF.1/MACSEC Test #4

Item	Data

Test Assurance Activity	If "**Cause Key Server to generate a new group CAK...**" is selected, the evaluator shall connect to the PAE of the TOE, set the management function specified in the ST (e.g., set ieee8021XKeyCreateNewGroup to true), and observe that the TOE distributes a new group CAK. **TD0512 has been applied.**
Test Steps & Expected Test Results	N/A – The TOE does not generate a group CAK.
Pass/Fail with Explanation	N/A – The TOE does not generate a group CAK.

6.7.26 FPT_FLS.1(2)/SelfTest Test #1

Item	Data
Test Assurance Activity	The following test may require the vendor to provide access to a test platform that provides the evaluator with the ability to modify the TOE internals in a manner that is not provided to end customers: Test 1: The evaluator shall modify the TSF in a way that will cause a self-test failure to occur. The evaluator shall determine that the TSF shuts down and that the behavior of the TOE is consistent with the operational guidance. The evaluator shall repeat this test for each type of self-test that can be deliberately induced to fail. For TOEs with redundant failover capability, the evaluator shall determine that the failed components shut down and the behavior of the TOE is consistent with the operational guidance. For each component, the evaluator shall repeat each type of self-test that can be deliberately induced to fail. ***TD0190 has been applied.***

Test Steps & Expected Test Results	• NOTE: This test requires a specially crafted set of images from the product vendor
	• For each type of self-test, deliberately induce the TOE to fail using the specialty image. The following self-tests require a demonstrated failure:
	  ○ AES Known Answer Test and verify the evidence with the console output
	TOE console output showing cipher AES Known Answer Test failure using the specialty image.
	  ○ GCM Known Answer Test and verify the evidence with the console output
	TOE console output showing cipher GCM Known Answer Test failure using the specialty image.
	  ○ CCM Known Answer Test and verify the evidence with the console output
	TOE console output showing cipher CCM Known Answer Test failure using the specialty image.
	  ○ CMAC Known Answer Test and verify the evidence with the console output
	TOE console output showing cipher CMAC Known Answer Test failure using the specialty image.
	  ○ RSA Signature Known Answer Test and verify the evidence with the console output
	TOE console output showing cipher RSA Known Answer Test failure using the specialty image.
	  ○ DRBG Known Answer Test and verify the evidence with the console output

	TOE console output showing DRBG Known Answer Test failure using the specialty image. ○ SHA-1/256/512 Known Answer Test and verify the evidence with the console output TOE console output showing SHA-1/256/512 Known Answer Test failure using the specialty image. ○ HMAC-SHA- 1/256/384/512 Known Answer Test and verify the evidence with the console output TOE console output showing HMAC-SHA- 1/256/384/512 Known Answer Test failure using the specialty image. ○ Software integrity test and verify the evidence with the console output TOE console output showing Software integrity test failure using the specialty image.
Pass/Fail with Explanation	Pass. The evaluator repeated the test for each type of self-test that was deliberately induced to fail, and TOE's behavior was consistent with each self-failure test. The TOE meets the test requirements.

6.7.27 FPT_RPL.1 Test #1

Item	Data
Test Assurance Activity	Before performing each test, the evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the Operational Environment sending enough traffic to see it working and verify the PN values increase for each direction. Test 1: The evaluator shall set up a MACsec connection with an entity in the Operational Environment. The evaluator shall then capture traffic sent from this remote entity to the TOE. The evaluator shall retransmit copies of this traffic to the TOE, in order to impersonate the remote entity where the PN values in the SecTag of these packets are less than the lowest acceptable PN for the SA. The evaluator shall observe that the TSF does not take an action in response to receiving these packets and that the audit log indicates that the replayed traffic was discarded.
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2 • Enter and create CKN and CAK value and verify them using command info

	TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established TOE logs showing the successful MACsec connection. • Capture and record MACsec from the peer to the TOE and retransmit the same traffic to the TOE using Acumen-MACsec tool Screenshot of the Acumen MACsec tool retransmitting captured MACsec packets. • Verify the TOE does not respond using packet capture A packet capture showing the TOE dropped the retransmitted MACsec packtes. • Verify the TOE does not respond using log TOE logs showing the count of dropped packets.
Pass/Fail with Explanation	Pass. The TOE discarded the replay traffic, and it did not respond to the replay packets. The TOE meets the test requirements.

6.7.28 FPT_RPL.1 Test #2

Item	Data
Test Assurance Activity	Before performing each test, the evaluator shall successfully establish a MACsec channel between the TOE and a MACsec-capable peer in the Operational Environment sending enough traffic to see it working and verify the PN values increase for each direction Test 2: The evaluator will capture frames during a MKA session and record the lowest PN observed in a particular time range. The evaluator will then send a frame with a lower PN, and then verify that this frame is dropped. The evaluator will verify that the device logged this event.
Test Steps & Expected Test Results	• Create connectivity association using command /configure macsec connectivity-association to configure the TOE to use MACsec with peer TOE command line output of the evaluator creating a macsec connectivity-association the TOE. • Create pre-shared key 1 using command static-cak pre-shared-key 1 encryption-type aes-128-cmac create TOE command line output of the evaluator creating PSK 1 • Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Create pre-shared key 2 using command static-cak pre-shared-key 2 encryption-type aes-256-cmac create TOE command line output of the evaluator creating PSK 2

	• Enter and create CKN and CAK value and verify them using command info TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Configure the required port to link the macsec connectivity association using command /configure port 1/1/1 ethernet dot1x macsec TOE command line output of the configuration used to link the macsec connectivity on the TOE. • Configure the sub port and ca-name with putting required values TOE command line output of the command string that the TOE uses to create CKN and CAK values. • Activate the sub-port using no shutdown command and save the config using /admin save TOE command line output of the evaluator activating the sub-port. • Verify the MACsec connection is established TOE logs showing the successful MACsec connection. • Using Acumen-MACsec tool capture and record MACsec from the peer to the TOE and retransmit the same traffic to the TOE Screenshot of the Acumen MACsec tool retransmitting captured MACsec packets. • Verify the TOE does not respond using packet capture A packet capture showing the TOE dropped the retransmitted MACsec packtes. • Verify the TOE does not respond using log TOE logs showing the count of dropped packets.
Pass/Fail with Explanation	Pass. The TOE dropped the frame with lower PN. The TOE meets the test requirements.

7 Security Assurance Requirements

7.1 ADV_FSP.1 Basic Functional Specification

7.1.1 ADV_FSP.1

7.1.1.1 ADV_FSP.1 Activity 1

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it describes the purpose and method of use for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the purpose and method of use for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.2 ADV_FSP.1 Activity 2

Objective	The evaluator shall examine the interface documentation to ensure it describes the purpose and method of use for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to develop a mapping of the interfaces to SFRs. The evaluator examined the entire AGD. Each Guidance Evaluation Activity is associated with a specific SFR. The Evaluation Findings for each Guidance Evaluation Activity identify the relevant interfaces, thus providing a mapping. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.1.1.3 ADV_FSP.1 Activity 3

Objective	The evaluator shall check the interface documentation to ensure it identifies and describes the parameters for each TSFI that is identified as being security relevant.
Evaluator Findings	The evaluator examined the AGD (interface documentation) to verify that it identifies and describes the parameters for each TSFI that is identified as being security relevant. The evaluator examined the entire AGD. The evaluator verified the AGD describes the parameters for each security relevant TSFI by verifying the AGD satisfies all of the Guidance Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2 AGD_OPE.1 Operational User Guidance

7.2.1 AGD_OPE.1

7.2.1.1 AGD_OPE.1 Activity 1

Objective	The evaluator shall ensure the Operational guidance documentation is distributed to Security Administrators and users (as appropriate) as part of the TOE, so that there is a reasonable

	guarantee that Security Administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration.
Evaluator Findings	The evaluator checked the requirements below are met by the guidance documentation. Guidance documentation shall be distributed to administrators and users (as appropriate) as part of the TOE, so that there is a reasonable guarantee that administrators and users are aware of the existence and role of the documentation in establishing and maintaining the evaluated configuration. Upon investigation, the evaluator found that the CC guidance will be published with the CC certificate on www.niap-ccevs.org.. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.2 AGD_OPE.1 Activity 2

Objective	The evaluator shall ensure that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	The evaluator ensured that the Operational guidance is provided for every Operational Environment that the product supports as claimed in the Security Target. The section titled Supported Platforms of the AGD was used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are those described in [ST], and lists all TOE platforms in [AGD] section 1.3, table 1 – TOE Physical Boundary Components Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.3 AGD_OPE.1 Activity 3

Objective	The evaluator shall ensure that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.
Evaluator Findings	The evaluator ensured that the Operational guidance contains instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. While performing the Guidance Evaluation Activities for the cryptographic SFRs, the evaluator ensured guidance contained the necessary instructions for configuring the cryptographic engines. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.4 AGD_OPE.1 Activity 4

Objective	The evaluator shall ensure the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs.
Evaluator Findings	The entire AGD was used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section titled “Enabling CC-NDcPP Compliance” specifies features that are not assessed and tested by the EAs. The evaluator

	ensured the Operational guidance makes it clear to an administrator which security functionality and interfaces have been assessed and tested by the EAs. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.2.1.5 AGD_OPE.1 Activity 5 **[TD0536]**

Objective	In addition, the evaluator shall ensure that the following requirements are also met. a) The guidance documentation shall contain instructions for configuring any cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE. b) The documentation must describe the process for verifying updates to the TOE for each method selected for FPT_TUD_EXT.1.3 in the Security Target. The evaluator shall verify that this process includes the following steps: i) Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory). ii) Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes instructions that describe at least one method of validating the hash/digital signature. c) The TOE will likely contain security functionality that does not fall in the scope of evaluation under this cPP. The guidance documentation shall make it clear to an administrator which security functionality is covered by the Evaluation Activities.
Evaluator Findings	The evaluator verified the guidance documentation contains instructions for configuring any cryptographic engines in AGD_OPE.1 Activity #3. The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2. The evaluator examined the whole of the guidance, and verified that the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3 AGD_PRE.1 Preparative Procedures

7.3.1 AGD_PRE.1

7.3.1.1 AGD_PRE.1 Activity 1

Objective	The evaluator shall examine the Preparative procedures to ensure they include a description of how the Security Administrator verifies that the operational environment can fulfil its role to support the security functionality (including the requirements of the Security Objectives for the Operational Environment specified in the Security Target).
Evaluator Findings	The evaluator examined the Preparative procedures to ensure they include a description of how the administrator verifies that the operational environment can fulfil its role to support

	the security functionality. The evaluator reviewed [AGD] section 1.3 and determined that the OE of the TOE is fully described, in terms of how each OE component supports the operation of the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.2 AGD_PRE.1 Activity 2

Objective	The evaluator shall examine the Preparative procedures to ensure they are provided for every Operational Environment that the product supports as claimed in the Security Target and shall adequately address all platforms claimed for the TOE in the Security Target.
Evaluator Findings	The evaluator checked the requirements below are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that the guidance documentation describes each of the devices in the operating environment in [AGD] section 1.3, which conforms to the description in [ST]. [AGD] section 1.3 identifies and describes the specific 7750 series chassis' which are in-scope of the evaluation. The evaluator verified that the list is consistent with the TOE described in [ST] Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.3 AGD_PRE.1 Activity 3

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to successfully install the TSF in each Operational Environment.
Evaluator Findings	The evaluator checked the requirements are met by the preparative procedures. The entire AGD was used to determine the verdict of this work unit. Upon investigation, the evaluator found that AGD describes all of the functions necessary to install and configure the TOE to work in the target operating environment, including, • Configuring Administrative Accounts and Passwords • Configuring SSH and Console Connections • Configuring the Remote Syslog Server • Configuring Audit Log Options • Configuring Event Logging • Configuring a Secure Logging Channel • Configuring MACsec • Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.4 AGD_PRE.1 Activity 4

Objective	The evaluator shall examine the preparative procedures to ensure they include instructions to manage the security of the TSF as a product and as a component of the larger operational environment.

Evaluator Findings	The evaluator ensured the preparative procedures include instructions to manage the security of the TSF as a product and as a component of the larger operational environment. The entire AGD was used to determine the verdict of this work unit. The same commands, configurations, and interfaces used to install the TOE are also used for ongoing management, so this is satisfied by AGD_PRE.1 Activity #3. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.3.1.5 AGD_PRE.1 Activity 5

Objective	In addition, the evaluator shall ensure that the following requirements are also met. The preparative procedures must a) include instructions to provide a protected administrative capability; and b) identify TOE passwords that have default values associated with them and instructions shall be provided for how these can be changed.
Evaluator Findings	The evaluator ensured the preparative procedures include instructions to provide a protected administrative capability and changing default passwords. The sections 2 and 7.1 were used to determine the verdict of this work unit. The AGD describes changing the default password associated with the root account and configuring SSH for remote administration. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4 ALC Assurance Activities

7.4.1 ALC_CMC.1

7.4.1.1 ALC_CMC.1 Activity 1

Objective	When evaluating that the TOE has been provided and is labelled with a unique reference, the evaluator performs the work units as presented in the CEM.
Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.4.2 ALC_CMS.1

7.4.2.1 ALC_CMS.1 Activity 1

Objective	When evaluating the developer's coverage of the TOE in their CM system, the evaluator performs the work units as presented in the CEM.

Evaluator Findings	The evaluator verified that the ST, TOE and Guidance are all labeled with the same hardware versions and software. The information is specific enough to procure the TOE and it includes hardware models and software versions. The evaluator checked the TOE software version and hardware identifiers during testing by examining the actual machines used for testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.5 ATE_IND.1 Independent Testing – Conformance

7.5.1 ATE_IND.1

7.5.1.1 ATE_IND.1 Activity 1

Objective	The evaluator performs the CEM work units associated with the ATE_IND.1 SAR. Specific testing requirements and EAs are captured for each SFR in Sections 2, 3 and 4. The evaluator should consult Appendix 709 when determining the appropriate strategy for testing multiple variations or models of the TOE that may be under evaluation.
Evaluator Findings	The evaluator examined the TOE to determine that the test configuration is consistent with the configuration under evaluation as specified in the ST. Upon investigation, the evaluator found that each instance of the TOE used in testing was consistent with TOE description found in the Security Target. Additionally, the evaluator found that the TOE version is consistent with what was specified in the Security Target. The evaluator examined the TOE to determine that it has been installed properly and is in a known state. The details of the installed TOE and any configuration performed with the TOE are found in the separate Test Reports. The evaluator prepared a test plan that covers all of the testing actions for ATE_IND.1 in the CEM and in the SFR-related Evaluation Activities. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6 AVA_VAN.1 Vulnerability Survey

7.6.1 AVA_VAN.1

7.6.1.1 AVA_VAN.1 Activity 1 **[TD0564] [Labgram #116]**

Objective	The evaluator shall document their analysis and testing of potential vulnerabilities with respect to this requirement.
Evaluator Findings	The evaluator documented their analysis and testing of potential vulnerabilities with respect to this requirement. Public searches were performed against all keywords found within the Security Target and AGD that may be applicable to specific TOE components. This included protocols, TOE software version, and TOE hardware to ensure sufficient coverage under AVA. The evaluator searched the Internet for potential vulnerabilities in the TOE using the web sites listed below. The sources of the publicly available information are provided below. • https://nvd.nist.gov/vuln/search • https://cve.mitre.org/ • https://www.tenable.com/cve

	• http://www.zerodayinitiative.com/advisories • https://www.rapid7.com/db/vulnerabilities • https://www.nokia.com/networks/products/7750-service-router/ - Vendor Website The evaluator performed the public domain vulnerability searches using the following key words. The search was performed on March 24, 2021, May 3, 2021, June 5, 2021, June 24, 2021, August 5, 2021 and October 10, 2021. The evaluation team found no vulnerabilities were applicable to the TOE version or hardware. The list of keywords searched include: • Nokia • 7750 Service Router • 7750 SR-7 • 7750 SR-12 • 7750 SR-12e • 7750 SR-1e • 7750 SR-2e • 7750 SR-3e • 7750 SR-a4 • 7750 SR-a8 • TLS v1.2 • MACsec • SSH v2 • SRCM 3.1 • OpenSSL 1.1.1g • TCP • Nokia 7750 SR OS 20.10.R4 The evaluation lab examined each result provided from NVD and Exploit Search to determine if the current TOE version or component within the environment was vulnerable. Based upon the analysis, any issues found that were generated were patched in the TOE version and prior versions, mitigating the risk factor. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

7.6.1.2 AVA_VAN.1 Activity 2

Objective	The evaluator shall perform the following activities to generate type 4 flaw hypotheses:
	• Fuzz testing
	  ○ Examine effects of sending:
	  ▪ mutated packets carrying each 'Type' and 'Code' value that is undefined in the relevant RFC for each of ICMPv4 (RFC 792) and ICMPv6 (RFC 4443)
	  ▪ mutated packets carrying each 'Transport Layer Protocol' value that is undefined in the respective RFC for IPv4 (RFC 791) IPv6 (RFC 2460) should also be covered if it is supported and claimed by the TOE.

	Since none of these packets will belong to an allowed session, the packets should not be processed by the TOE, and the TOE should not be adversely affected by this traffic. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis. ○ Mutation fuzz testing of the remaining fields in the required protocol headers. This testing requires sending mutations of well- formed packets that have both carefully chosen and random values inserted into each header field in turn (i.e. testing is to include both carefully chosen and random insertion test cases). The original well-formed packets would be accepted as part of a normal existing communication stream and may still be accepted as valid packets when subject to the carefully chosen mutations (the individual packet alone would be valid although its contents may not be valid in the context of preceding and/or following packets), but will often not be valid packets when random values are inserted into fields. The carefully chosen values should include semantically significant values that can be determined from the type of the data that the field represents, such as values indicating positive and negative integers, boundary conditions, invalid binary combinations (e.g. for flag sets with dependencies between bits), and missing start or end values. Randomly chosen values may not result in well-formed packets but are included nonetheless to see whether they can lead to the device entering an insecure state. Any results that are unexpected (e.g., core dumps) are candidates for a flaw hypothesis.
Evaluator Findings	The evaluator documented the fuzz testing results with respect to this requirement. The evaluation lab examined each result from fuzz testing to determine if the TOE improperly processes packets. Based upon the analysis, no unexpected results occurred. Therefore, no Type 4 hypotheses were generated. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

8 Conclusion

The testing shows that all test cases required for conformance have passed testing.

End of Document