Assurance Activity Report for
Nokia 7705 SAR Series with SAR OS 21.10R5

Nokia 7705 SAR Series with SAR OS 21.10R5 Security Target
Version 1.4

collaborative Protection Profile for Network Devices
Version 2.2e

AAR Version 1.3, September 28, 2023

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:
Acumen Security, LLC
Shehan Dissanayake
Shivani Birwadkar
Minal Wankhede
Yogesh Pawar

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
1.0	24/05/2023	Initial Release
1.1	12/08/2023	Minor updates to address ECR comments
1.2	15/09/2023	Update to section 7.6, AVA_VAN search date
1.3	28/09/2023	Update to section 5.2.2 and section 8.2

Contents

`

1 TOE Overview

The TOE is the Nokia 7705 Service Aggregation Router (SAR) series with SAR OS 21.10R5 consisting of the following versions:

- Nokia 7705 SAR-18,
- Nokia 7705 SAR-8,
- Nokia 7705 SAR-X,
- Nokia 7705 SAR-H,
- Nokia 7705 SAR-W,
- Nokia 7705 SAR-Wx,
- Nokia 7705 SAR-Hc, and
- Nokia 7705 SAR-Ax

Versions of the TOE differ in form factor, networking capacity, and processing capacity.

The TOE Description section provides an overview of the TOE architecture, including physical boundaries, security functions, and relevant TOE documentation and references.

2 Assurance Activities Identification

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

3 Test Equivalency Justification

This section provides a testing equivalency analysis for the Nokia SAR OS 21.10R5. This section also describes the intended operational environment of the TOE, and the functional and assurance requirements that the TOE meets. It satisfies all the criterion to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].

3.1 Architectural Description

The Nokia SAR OS 21.10R5 comprise the TOE. All the possible TOE chassis are listed below:

- Nokia 7705 SAR-18,
- Nokia 7705 SAR-8,
- Nokia 7705 SAR-X,
- Nokia 7705 SAR-H,
- Nokia 7705 SAR-W,
- Nokia 7705 SAR-Wx,
- Nokia 7705 SAR-Hc, and
- Nokia 7705 SAR-Ax

The hardware is comprised of the following: Nokia 7705 SAR-18, 7705 SAR-8, 7705 SAR-X, 7705 SAR-H, 7705 SAR-W, 7705 SAR-Wx, 7705 SAR-Hc, and 7705 SAR-Ax. The software is comprised of the Nokia SAR OS 21.10R5.

The TOE consists of hardware, software, and security guidance documentation. TOE Hardware is contained in the TOE chassis. Variants of the TOE chassis differ in the physical size, precise hardware configuration, the number of network card slots and network interfaces, and throughput capacity. Some variants include network card slots which may be used for configuring the network ports of the product to precisely match the needs of a specific application.

The TOE is deployed inside a secure data center or other premises where physical access is effectively controlled. This ensures that only authorized personnel gain physical access to the TOE. Logical access may be through the management station or through the network interfaces. A management station may be local or remote. In addition to the management stations, a CA/CRL Server, AAA Server, Syslog Server and Update Server may be deployed in the same network with the TOE. Access methods to the different management stations and servers are different as are the protocols for protecting network traffic between them and the TOE.

3.2 Equivalency Analysis

The following equivalency analysis provides 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].

3.2.1 Platform/Hardware Dependencies

The hardware is comprised of the following models: Nokia 7705 SAR-18, 7705 SAR-8, 7705 SAR-X, 7705 SAR-H, 7705 SAR-W, 7705 SAR-Wx, 7705 SAR-Hc, and 7705 SAR-Ax

Hardware Models	7705 SAR-18	7705 SAR-8	7705 SAR-X	7705 SAR-H	7705 SAR-Hc	7705 SAR-W	7705 SAR-Wx	7705 SAR-Ax
Slots/ Variants	8 slots	18 slots	2 variants	2 variants	1 variant	1 variant	2 variants	7705 SAR-Ax
Rack Units	10RU	2RU	1RU	1.5RU	DIN rail-mountableWall-mountablePanel-mountable	1RU	Pole-mountable Wall-mountable Cable strand-mountable	1 variant
Dimensions	• Height: 8.9 cm (3.5 in.) • Depth: 25.4 cm (10 in.) • Width: 43.9 cm (17.3 in.)	• Height: 44.5 cm (17.5 in.) • Depth: 30 cm (10 in.) • Width: 43.9 cm (17.3 in.)	• Height: 4.37cm (1.72 in) •Depth: 25.4cm (10 in) • Width: 44.2 cm (17.4 in)	• Height: 1.7RU (76.2 mm) (3 in) • Width: 254 mm (10 in) • Depth: 279.4 mm (11 in)	• Height: 17.8 cm (7 in) • Width: 9.14 cm (3.6 in) • Depth: 15.24 cm (6 in)	• Height: 6.6 cm (2.6 in) • Depth: 25.4 cm (10 in) • Width: 38.1 cm (15 in)	• Height: 9.7 cm (3.8 in) • Depth: 16.5 cm (6.5in) • Width: 35.6 cm (14 in)	• Height: 1 RU 4.3 cm (1.7 in) • Depth: 20.1 cm (7.9 in) • Width: 43.79 cm (17.24 in)
Memory	140 Gb/s HD	12 Gb/s HDSAR-8 Shelf V2: 60 Gb/s HD	54 Gb/s HD	8 Gb/s HD	5 Gb/s HD	10 Gb/s HD	10 Gb/s HD	10 Gb/s (HD)
CPU	Cavium OCTEON Plus CN5640	Cavium OCTEON II CN6335	Cavium OCTEON II CN6640	Cavium OCTEON Plus CN5020	Cavium OCTEON II CN6020	Cavium OCTEON Plus CN5010	Cavium OCTEON II CN6020	Cavium OCTEON II CN6020

3.2.2 Software/OS Dependencies:

This category of differences is only applicable if the TOE is installed on an OS outside of the TOE boundary. In this case, all software including the OS is included in SAR-OS and within the TOE boundary. There are no specific dependencies on the OS since the TOE will not be installed on different OSs. The image used on Nokia 7705 SAR-18, 7705 SAR-8, 7705 SAR-X, 7705 SAR-H, 7705 SAR-W, 7705 SAR-Wx, 7705 SAR-Hc, and 7705 SAR-Ax is SAR-OS.

Result: All platforms are equivalent

3.2.3 Differences in Libraries Used to Provide TOE Functionality

All software binaries compiled in the TOE software are identical and have the same version numbers. There are no differences between the included libraries. Of note, the TOE uses the same CAVP validated crypto module to provide its cryptographic functionality. This is the same across platforms.

Result: All platforms are equivalent

3.2.4 TOE Management Interface Differences

The TOE is managed locally or remotely. In both methods, the administrative interface is the Command Line Interface (CLI). These management options are available on all hardware platforms regardless of the configuration. There is no difference in the management interface for any platform.
Result: All platforms 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.
Result:

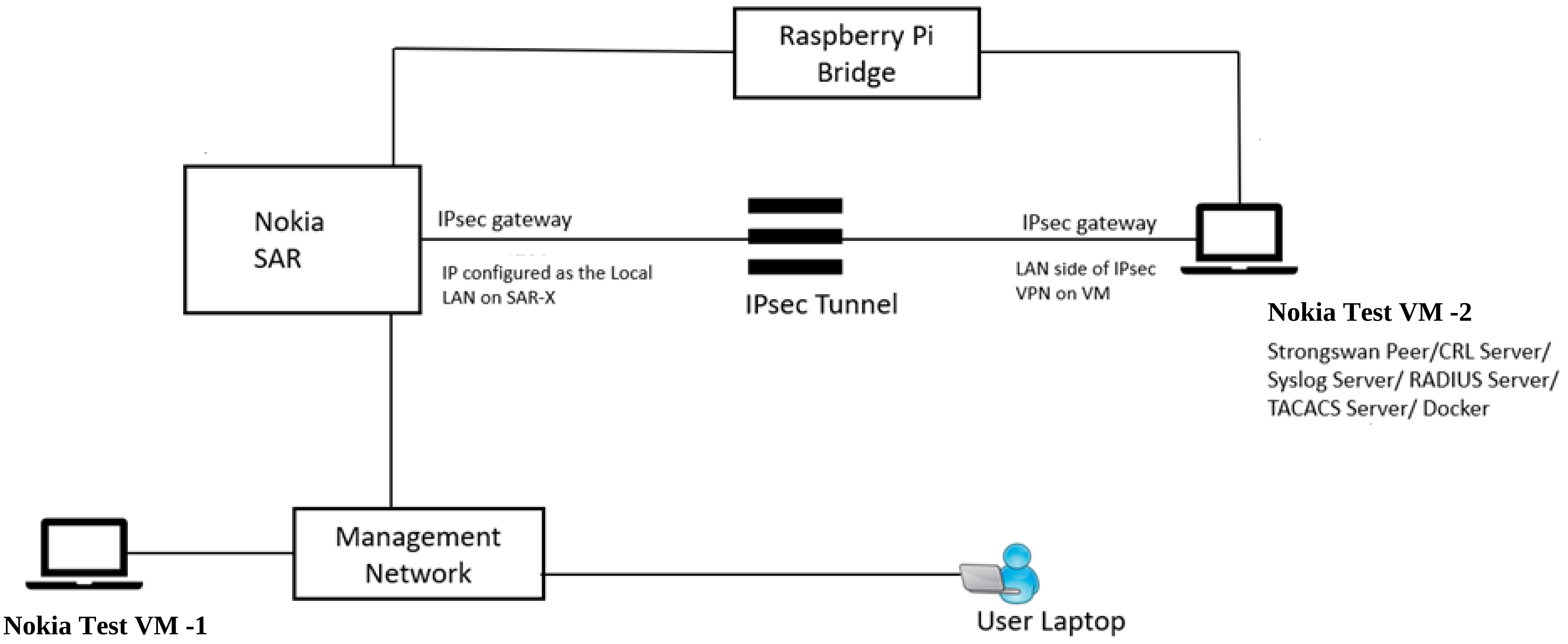
- There are no security functional differences between platforms in a series.
- All appliances are equivalent.

3.3 Recommendations/Conclusions

Based on the equivalency rationale listed above, full set of testing will be performed on the following subset:

- SAR-W: Cavium OCTEON Plus CN5010
- SAR-X: Cavium OCTEON II CN6640

4 Test Bed Descriptions


Raspberry Pi Bridge
Nokia SAR
IPsec gateway
IP configured as the Local LAN on SAR-X
IPsec Tunnel
IPsec gateway
LAN side of IPsec VPN on VM
Nokia Test VM -2
Strongswan Peer/CRL Server/ Syslog Server/ RADIUS Server/ TACACS Server/ Docker
Management Network
Nokia Test VM -1
User Laptop

Name	OS	Function	Protocols	Time	Tools (version)
7705 SAR-X & 7705 SAR-W	Nokia SAR OS 21.10R5	TOE	SSH IPsec	Manually set and verified	
Raspberry Pi Bridge	Ubuntu 4.14.71	Packet Capture	IPsec	Manually set and verified	tcpdump version (4.9.3) libpcap version (1.8.1)
Test VM1	Ubuntu 5.4.0	Packet Capture	SSH	Manually set and verified	tcpdump version (4.9.3) libpcap version (1.9.1)
Test VM2	Ubuntu 5.4.0	Strongswan/ RADIUS server/ Syslog server/ TACACS server/ Docker	SSH IPsec NAT-T IP	Manually set and verified	Syslog-ng version (3.25.1) StrongSwan Version (5.9.2)
Test user Laptop	Windows 10 pro	Test workstation	SSH	Manually set and verified	MobaXtermv21.3, XCA 2.1.1, WinSCP 5.19.6 Wireshark 3.4.8

All testing was carried out at the Acumen Security offices located in 2400 Research Blvd Suite #395, Rockville, MD 20850. Testing occurred from May 2022 to May 2023. The TOE was in a physically protected, access controlled, designated test lab with no unattended entry/exit ways. At the start of each day, the test bed was verified to ensure that it was not compromised. All evaluation documentation was always kept in a secure repository.

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 **FAU_GEN.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE produces audit events for start-up and shutdown of the audit functions as well as the following: administrative login and logout; password resets; changes to the TOE data related to configuration; the generation, import of, changing, or deletion of cryptographic keys. Audit records include the identity of the administrator initiating the cryptography related events such as, key generation (e.g. RSA), import, or deletion. The audit record contains the information such as, the identity of the key (unique name including the size and type), the date and time of the event, type of event, and the outcome of the event. 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 the sections titled **1.1 Overview of Log Events** and **2 7705 SAR Log Event** in the AGD titled **Log Events Guide** to verify that it provides an example of each auditable event required by FAU_GEN.1. Upon investigation, the evaluator found that the tables **'Table 1 Log Event Element Descriptions', 'Table 609 cli_user_login properties', 'Table 1189 tmnxUserPasswordChangedByAdmin properties'**, '**Table 2 cli_config_io properties', 'Table 1123 tmnxCertImport properties'** and **'Table 1124 tmnxCertKeyPairGen properties'** contains a listing and description of each of the fields in generated audit records that contain the information required in FAU_GEN.1.2, as well as an example audit record. The evaluator next compared this list of events to the auditable events listed in the NDcPP.

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

5.1.1.3 FAU_GEN.1 Guidance 2

<table>
<tr><td>Objective</td><td>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.</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator examined each 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 first examined the entirety of both AGDs to determine what administrative commands are associated with each administrative activity. Upon investigation, the evaluator found that the following are applicable:
<table>
<tr><th>Administrative Activity</th><th>Method (Command/GUI Configuration)</th><th>Section</th></tr>
<tr><td>Startup/shutdown of the Audit Function</td><td>A series of CLI commands are provided for configuration</td><td>5.10.7 Configuring a Syslog Target</td></tr>
<tr><td>Terminating session</td><td>logout</td><td>3.11.2.1 Basic CLI Commands</td></tr>
<tr><td>Display system information</td><td>show version</td><td>3.8.5 History</td></tr>
<tr><td>Login Banner</td><td>config>system>login-control</td><td>3.10.2.1.15 Login Control Commands</td></tr>
<tr><td>Session Termination</td><td><b>Syntax</b> idle-timeout {minutes | disable}
no idle-timeout
<b>Context</b> config>system>login-control</td><td>3.10.2.1.15 Login Control Commands</td></tr>
</table>
</td></tr>
</table>

Lockout configuration	**Syntax** attempts count [time minutes1] [lockout minutes2] no attempts **Context** config>system>security>password	3.10.2.1.6 Password Commands
Setting Password Length	config>system>security>password>complexity-rules	3.10.2.1.6 Password Commands
Creating Users	[no] user user-name	3.10.2.1.8 User Management Commands
Management of Crypto Keys	rsa config>system>security>user>public-keys	3.10.2.1.8 User Management Commands
Clock Management	admin set-time date time	6.10.6.2 Set-time, 6.13.2.1.5 System Time Commands
Creation of the CSR	**cert-request ca** *ca-profile-name* **current-key** *key-filename* **current-cert** *cert-filename* [**hash-alg** *hash-algorithm*] **newkey** *key-filename* **subject-dn** *subject-dn* **save-as** save-path-of-result-cert	8.10.2.2.1 X.509 and Certificate Commands
Authenticating the Certificate Authority	**Syntax** auth-method {psk | cert-auth} no auth-method **Context** config>ipsec>ike-policy **Syntax** trust-anchor-profile name [create] no trust-anchor-profile name **Context** config>ipsec	8.10.2.2.3 IPSec PKI Commands
Configuring a Revocation Mechanism	A series of CLI commands are provided for configuration	8.10.2.2.5 Automatic CRL Update Commands

Configuring SSH	A series of CLI commands are provided for configuration	3.10.2.1.13 SSH Commands
Configuring IKE/IPsec	A series of CLI commands are provided for configuration	8.10.2.1 IPSec Configuration Commands, 8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands

Next, the evaluator examined each of the test cases and identified test cases which exercised the above referenced functionality. The audit record associated with the configuration was captured. The following table identifies the test cases in which audit records for those configurations can be found:

Administrative Activity	**Method (Command/GUI Configuration)**	**Test Case(s)**
Startup/shutdown of the Audit Function	A series of CLI commands are provided for configuration	FAU_GEN.1 T1
Terminating session	logout	FTA_SSL.4 T1 FTA_SSL.4 T2
Display system information	show version	FPT_TUD_EXT.1 T1
Login Banner	config>system>login-control	FTA_TAB.1 T1
Session Termination	**Syntax** idle-timeout {minutes | disable} no idle-timeout **Context** config>system>login-control	FTA_SSL_EXT.1 T1 FTA_SSL.3 T1
Lockout configuration	**Syntax** attempts count [time minutes1] [lockout minutes2] no attempts **Context** config>system>security>password	FIA_AFL.1 T1 FIA_AFL.1 T2

Setting Password Length	config>system>security>password>complexity-rules> minimum-length	FIA_PMG_EXT.1 T1
Creating Users	[no] user user-name	FIA_PMG_EXT.1 T1
Management of Crypto Keys	rsa config>system>security>user>public-keys	FMT_MTD.1/CryptoKeys T2
Clock Management	admin set-time date time	FPT_STM_EXT.1 T1
Creation of the CSR	**cert-request ca** *ca-profile-name* **current-key** *key-filename* **current-cert** *cert-filename* [**hash-alg** *hash-algorithm*] **newkey** *key-filename* **subject-dn** *subject-dn* **save-as** save-path-of-result-cert	FIA_X509_EXT.3 T1
Authenticating the Certificate Authority	**Syntax** auth-method {psk | cert-auth} no auth-method **Context** config>ipsec>ike-policy **Syntax** trust-anchor-profile name [create] no trust-anchor-profile name **Context** config>ipsec	FIA_X509_EXT.1.1/Rev T1
Configuring a Revocation Mechanism	A series of CLI commands are provided for configuration	FCS_IPSEC_EXT.2 T1
Configuring SSH	A series of CLI commands are provided for configuration	FCS_SSHS_EXT.1.4 T1
Configuring IKE/IPsec	A series of CLI commands are provided for configuration	FCS_IPSEC_EXT.1.1 T1

	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 **FAU_STG_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE is a standalone TOE that is configured to export audit data to a specified, external audit server. The TOE protects communications with an external audit server via IPSEC. 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 **FAU_STG_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 maintains a circular buffer of a maximum of 3000 audit records which is exported to a syslog server in real time. If for any reason the number of entries exceeds the capacity (i.e. the maximum number of audit records), the circularity of the buffer ensures that the oldest entries are overwritten when new entries are generated and stored. Only authorized Administrators may access the audit records, unprivileged users have no access rights to the log files. 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 **FAU_STG_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 maintains a circular buffer of a maximum of 3000 audit records which is exported to a syslog server in real time. If for any reason the number of entries exceeds the capacity (i.e. the maximum number of audit records), the circularity of the buffer ensures that the oldest entries are overwritten when new entries are generated and stored. 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 **FAU_STG_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 maintains a circular buffer of a maximum of 3000 audit records which is exported to a syslog server in real time. If for any reason the number of entries exceeds the capacity (i.e. the maximum number of audit records), the circularity of the buffer ensures that the oldest entries are overwritten when new entries are generated and stored. 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 **FAU_STG_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: **"The TOE maintains a circular buffer of a maximum of 3000 audit records which is exported to a syslog server in real time. If for any reason the number of entries exceeds the capacity (i.e. the maximum number of audit records), the circularity of the buffer ensures that the oldest entries are overwritten when new entries are generated and stored."** 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 the section titled **'Using a Secure Audit Server'** in the AGD **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'** 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 guidance document states that: **"If an authorized administrator wants to back up logs to a syslog server, then protection must be provided for the syslog server communications which can be done with a syslog server operating as an IPsec peer of the TOE and the log records being tunneled over that connection."**

	In addition, the section **'Cryptographic Protocols',** sub-section **'IPSec'** provides detailed information on the protocols to be used of the secure channel and also provides configuration steps. This guidance document also provides information on how to configure the syslog parameters in the section '**Using a Secure Audit Server'.** 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 the sections titled **5.2.6 Syslog, 5.10.7 Configuring a Syslog Target, 5.11 Log Management Tasks, 5.12.2.1.9 Logging Destination Command, 5.11.5 Modifying a Syslog ID** and **5.11.6 Deleting a Syslog ID** in the AGD titled **System Management Guide** 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: **5.2.6 Syslog** An event log can be configured to send events to one syslog destination. Syslog destinations have the following properties: • syslog server IP address (IPv4 or IPv6) • the UDP port used to send the syslog message • the Syslog Facility Code • the Syslog Severity Threshold (0 to 7) (events exceeding the configured level will be sent) **5.12.2.1.9 Logging Destination Command** to syslog Syntax to syslog syslog-id

	Context config>log>log-id Description This command instructs the alarms and traps to be directed to a specified syslog. To remain consistent with the standards governing syslog, messages to syslog are truncated to 1 kbyte. The command is one of the to commands used to specify the log ID destination. A to command is mandatory when configuring a log destination. The source of the data stream must be specified in the from command prior to configuring the destination with the to command. In addition to above, the AGD **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’,** section **‘Using a Secure Audit Server’** states the following: **“When a Syslog server is configured on the TOE, the generated audit events are simultaneously sent to the external server and the local logging buffer.”** 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	The evaluator examined the sections titled **5.2.3 Memory Logs** and **5.12.2.1.9 Logging Destination Commands** in the AGD titled **System Management Guide** and the section titled **5.2.1.3 FAU_STG_EXT.1 Protected Audit Event Storage** in the Security Target to verify that it describes all possible configuration options for FAU_STG_EXT.1.3 and the resulting behavior of the TOE for each possible configuration. Upon investigation, the evaluator found that the Security Target states that: The TSF shall [*overwrite previous audit records according to the following rule: [overwrite the oldest logs]*] when the local storage space for audit data is full. And the AGD titled **System Management Guide** states that: **5.2.3 Memory Logs**

	A memory log is a circular buffer. When the log is full, the oldest entry in the log is replaced with the new entry. When a memory log is created, the specific number of entries it can hold can be specified; otherwise, it will assume a default size. An event log can send entries to a memory log destination. **5.12.2.1.9 Logging Destination Commands** to memory Syntax to memory [size] Context config>log>log-id Description This command instructs the events selected for the log ID to be directed to a memory file. A memory file is a circular buffer. Once the file is full, each new entry replaces the oldest entry in the log. 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 **FCS_CKM.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the key sizes supported by the TOE. Upon investigation, the evaluator found that the TSS states that: **To support the cryptographic protocols, the TOE uses RSA schemes using cryptographic key sizes of 2048-bit that meet the following:** **1. RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3;** **2. FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3 and RFC 3526”** 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 the section **‘Authentication’**, sub-section **‘Configure SSH Public Keys’** and Section **‘Cryptographic Protocols’,** sub-sections ‘**SSH’** and **‘IPSec’** in the AGD titled **“NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide”** 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 states that: **Configure SSH Public Keys** Before SSH can be used with PKI, a public/private key pair must be generated. This is typically supported by the SSH client software. For example, PuTTY supports a utility called PuTTYGen that will generate key pairs. The 7705 SAR currently supports Rivest, Shamir, and Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) user public keys. The RSA public key is supported up to 4096 bits and the ECDSA public key is supported up to NIST P-521. **Note**: *Only the RSA keys are to be used in the CC evaluated configuration because the ST does not claim ECDSA keys.* If the client is using PuTTY, they first generate a key pair using PuTTYGen. The user sets the key type to SSH-2 RSA and sets the number of bits to be used for the key. The user can also configure a passphrase that is used to store the key locally in encrypted form. If the passphrase is configured, it acts as a password for the private key and the user must enter the passphrase in order to use the private key. If a passphrase is not used, the key is stored in plain text locally. This section along with the sub-section **‘SSH’** provide detailed configuration steps on how to configure the TOE to use the selected key generation schemes and key sizes for user authentication for SSH. In addition, the sub-section **‘IPSec’** in the section **‘Cryptographic Protocols’** in the same document provides detailed guidance on how to configure the TOE to use the keys in the IPSec tunneling protocol. 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: RSA - #C2023 and #C2024 FFC Safe-Prime - #A3133 and #A3134 Detailed information on the CAVP certificate mapping can be found in the '**section 8 CAVP Mapping**' below. 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]**

<table>
<tr><td>Objective</td><td>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.</td></tr>
<tr><td>Evaluator Findings</td><td>

The evaluator examined the **FCS_CKM.2** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that:

The TOE performs cryptographic key establishment in accordance with key establishment schemes that are conformant to the following:

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

<table>
<tr><th>Scheme</th><th>SFR</th><th>Services</th></tr>
<tr><td>FFC-Safe Primes /DHG14
FFC-Safe Primes /DHG16</td><td>FCS_SSHS_EXT.1</td><td>Administration</td></tr>
<tr><td>FFC-Safe Primes /DHG14
FFC-Safe Primes /DHG15</td><td>FCS_IPSEC_EXT.1</td><td>Administration</td></tr>
<tr><td>RSA</td><td>FCS_SSHS_EXT.1</td><td>Administration</td></tr>
<tr><td></td><td>FCS_IPSEC_EXT.1</td><td>Audit server,
Authentication server</td></tr>
</table>

</td></tr>
</table>

	TSS also states to refer to Table 5 of the ST for CAVP mapping. Evaluator verified that the Table 5 contains relevant information for the claimed key establishment schemes. 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 the section titled **3.10.2.1.13 SSH Commands** in the AGD titled **System Management Guide** and sections titled **8.1.1.5 IPSec Security Policy, IKE Policy, and IPSec Transform** and **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** in the AGD titled **Services Guide** 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: **3.10.2.1.13 SSH Commands** kex Syntax kex index name kex-name no kex index Context config>system>security>ssh>client-kex-list config>system>security>ssh>server-kex-list Description This command configures the list of preferred KEX algorithms that are negotiated by the client and server using an SSHv2 phase one handshake. **Note:** If a 7705 SAR node is running in FIPS-140-2 mode: • SSHv1 is not supported • The following KEX algorithm is not available: diffie-hellman-group1-sha1 The ***no*** form of this command removes the specified KEX index. Removing all the indexes from a client or server list results in an empty list, and any KEX algorithm the client or server brings to the SSHv2 negotiation will be rejected. **Default:** no kex

	Parameters index — the index of the KEX algorithm in the list. The list is ordered from highest to lowest. Values 1 to 255 kex-name — the KEX algorithm for computing the shared secret key Values diffie-hellman-group16-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1 Based on these findings, this assurance activity is considered satisfied. **8.1.1.5 IPSec Security Policy, IKE Policy, and IPSec Transform** An IKE policy defines how the 7705 SAR encrypts and authenticates an IPSec tunnel that uses that policy. Its configuration includes specifics on Diffie-Hellman key derivation algorithms, encryption, and authentication protocols to be used for establishing phase 1 and phase 2 security associations, and so on. **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** dh-group Syntax dh-group {1 | 2 | 5 | 14 | 15} no dh-group Context config>ipsec>ike-policy Description This command specifies which Diffie-Hellman group is used to calculate session keys: • Group1: 768 bits • Group2: 1024 bits • Group5: 1536 bits • Group14: 2048 bits • Group15: 3072 bits More bits provide a higher level of security but require more processing. The no form of the command returns the parameter to its default value (Group2).

	Default no dh-group (Group2). In addition to above details, the Common Criteria guide titled “**NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide”** also provides the same information. The CC guide also has the following instructions for the administrators on limitations of the DH Groups to be used in the IPSec tunnel configurations: **“Note:** *The DH Groups (1, 2, 5) should not be used in the CC evaluated configuration”*
Verdict	Pass

5.2.2.3 FCS_CKM.2 Test/CAVP 1

Objective	The evaluator shall verify the key establishment mechanisms supported by the TOE.
Evaluator Findings	CAVP Certs: #**A3133** and **#A3134** Detailed information on the CAVP certificate mapping can be found in the ‘**section 8 CAVP Mapping**’ below. 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 section titled **Cryptographic Key Destruction** in the Security Target 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 states that:

The TOE destroys all cryptographic keys using the following methods:

- For plaintext keys in volatile storage, the TOE uses a single overwrite consisting of zeroes.
- For all plaintext keys in non-volatile storage, the TOE destroys keys via invocation of an interface provided by a part of the TOE that instructs TOE to destroy the abstraction that represents the key.

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

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
SSH Private host key	SSH Server host private key stored in the local file system	Volatile memory when used, file system for persistent storage	Single overwrite with zeros in volatile memory, file erasure in persistent storage
SSH Session key	Session key loaded into memory to complete a SSH session establishment	Volatile memory	Single overwrite with zeros
RNG state	Internal state and seed key of the DRBG	Volatile memory	Handled by kernel, overwritten with zeros at the boot-up
IKE Private host key	Private authentication used by IKE	In volatile memory when used, in file system when persistently stored	Single overwrite with zeros in volatile memory, not erased when persistently stored
IKE-SKEYID	IKE master secret for deriving IKE and IPsec ESP Session keys	Volatile memory	Erased when a tunnel goes down or zeroized at reboot
IKE Session key	IKE Session keys	Volatile memory	Erased when a tunnel goes down or zeroized at reboot

ESP Session key	ESP Session keys	Volatile memory	Erased when a tunnel goes down or zeroized at reboot
IKE-DH Private exponent	Ephemeral DH private exponent used in IKE	Volatile memory	Erased when a tunnel goes down or zeroized at reboot
SW Integrity key	The key used in the HMAC for verifying the TOE Software integrity.	Shipped with the software image package, resides in the same directory with the software image files. The location is pointed to by the BOF (boot options file) and may be Compact Flash (CF) or an FTP location outside of the TOE.	Replaced with a new value when a new software image package is loaded.

The Evaluator found that the descriptions of keys and storage locations is consistent with the functions carried out by the TOE.

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 **FCS_CKM.4** entry in the section titled **TOE Summary Specification** and the section titled **Cryptographic Key Destruction** in the Security Target 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 table provided information on keys stored in non- volatile memory including a description of the interfaces used to destroy keys. 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 section titled **Cryptographic Key Destruction** in the Security Target 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 states that no keys are 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 section titled **Cryptographic Key Destruction** in the Security Target 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 TOE zeroizes all secrets, keys, and associated values when they are no longer required. Hence no circumstances were found where destruction may be prevented or delayed. 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 verified that ST does not claim the use of 'a value that does not contain any CSP' to overwrite keys. 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 each AGD and Security Target 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 no items that did not meet conformance to the key destruction requirement. 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 **FCS_COP.1/DataEncryption** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that: The TOE supports AES encryption and decryption conforming to ISO 18033-3, ISO 10116 and ISO 19772. The TOE provides AES encryption and decryption in support of SSHv2 for secure communications. The AES key sizes supported for SSH are 128 bits and 256 bits and the AES modes supported are: CBC and CTR.

	In addition, AES_CBC is used in as a Cryptographic Algorithm selection for ESP protocol. The key sizes are 128-bits, 192-bits, and 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 the section titled **‘Cryptographic Protocols’ s** in the AGD titled “**NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide”** to verify that it provides 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. Upon investigation, the evaluator found that the AGD states that: **SSH server cipher algorithm configuration** • **cipher** **Syntax**: cipher *index* name *cipher-name* no cipher *index* **Context**: config>system>security>ssh>client-cipher-list config>system>security>ssh>server-cipher-list **Description:** This command configures the allowed SSH protocol version 1 or version 2 cipher that are available on the SSH client or server. Client cipher and server cipher lists are used to negotiate the best compatible cipher between the SSH client and SSH server. Client ciphers are used when the 7705 SAR node is acting as an SSH client; server ciphers are used when the 7705 SAR node is acting as an SSH server. The no form of this command deletes the specified cipher index. **Values For SSHv2:** **client ciphers:** aes128-ctr, aes192-ctr, aes256-ctr, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc **server ciphers:** aes128-ctr, aes192-ctr, aes256-ctr, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc **Note**: • *The blowfish-cbc, cast128-cbc, arcfour, and rijndael-cbc ciphers are not available if the 7705 SAR node is running in FIPS-140-2 mode.*

	• *The cryptographic keys - aes192-ctr and aes192-cbc are not to be used in the CC evaluated configuration because these two algorithms are not allowed for SSH in NDcPP 2.2e.* • *The protocol-version 1 is not available under FIPS-140-2 mode.* **Internet Key Exchange (IKE) and Transform Commands** • **encryption-algorithm** **Syntax**: encryption-algorithm {des | 3des | aes128 | aes192 | aes256} no encryption-algorithm **Context**: config>ipsec>ike-policy **Description**: This command specifies the encryption algorithm to use for the IKE session. The no form of the command returns the algorithm to its default value (aes128). **Default**: aes128 **Parameters**: des — configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. It should only be used when a strong algorithm is not available at both ends at an acceptable performance level. 3des — configures the 3-des algorithm for encryption. This is a modified application of the des algorithm that uses multiple des operations for more security. aes128 — configures the aes algorithm with a block size of 128 bits. This is the mandatory implementation size for aes. aes192 — configures the aes algorithm with a block size of 192 bits. This is stronger version of aes. aes256 — configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes. **Note:** *The des, and 3des algorithms are not to be used in the CC evaluated configuration.* 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: **#C2023 and C2024**

	Detailed information on the CAVP certificate mapping can be found in the '**section 8 CAVP Mapping**' below. 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 **FCS_COP.1/SigGen** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that: The TOE supports cryptographic signature services such as generation and verification using RSA Digital Signature Algorithm that meet the RSA scheme specified in FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PKCS1v1_5. The RSA key size supported is 2048 bits. RSA signature generation is used with SSH Public Key Authentication. 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 the section titled **8.7.6 Configuring X.509v3 Certificate Parameters** in the AGD titled **Services Guide** to verify that it provides 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. Upon investigation, the evaluator found that the AGD states that: Perform the following steps to configure certificate enrollment. Step 1. Generate a key: admin certificate gen-keypair cf3:/key_plain_rsa2048 size 2048 type

	rsa Step 2. Generate a certificate request: admin certificate gen-local-cert-req keypair cf3:/key_plain_rsa2048 subject-dn "C=US,ST=CA,CN=7705" file 7705_req.csr Step 3. Send the certificate request to CA-1 to sign and get the signed certificate. Step 4. Import the key: admin certificate import type key input cf3:/key_plain_rsa2048 output key1_rsa2048 format der Step 5. Import the signed certificate: admin certificate import type cert input cf3:/7705_cert.pem output 7705cert format pem. The same information was also found in the guidance document titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide',** section '**X.509 Certificates'**. 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: #**C2023** and **#C2024** Detailed information on the CAVP certificate mapping can be found in the '**section 8 CAVP Mapping**' below. 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 **FCS_COP.1/Hash** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that: The TOE supports Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. The hashing algorithms are used in SSH connections for secure communications. The following hashing algorithms are supported: SHA-1, SHA-256, SHA-384, and SHA-512. The message digest sizes supported are: 160, 256, 384, and 512 bits. 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 the sections titled **'IPSec'** in the AGD titled '**NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'** to verify that it presents any configuration that is required to configure the required hash sizes. Upon investigation, the evaluator found that the AGD states that: • **auth-algorithm** **Syntax:** auth-algorithm {md5 | sha1 | sha256 | sha384 | sha512} no auth-algorithm **Context:** config>ipsec>ike-policy **Description**: This command specifies which hashing algorithm to use for the IKE authentication function. The no form of the command returns the parameter to its default value. **Default**: sha1 **Parameters:** md5 — specifies the hmac-md5 algorithm for authentication sha1 — specifies the hmac-sha1 algorithm for authentication sha256 — specifies the sha256 algorithm for authentication

	sha384 — specifies the sha384 algorithm for authentication sha512 — specifies the sha512 algorithm for authentication **Note**: *The md5 algorithm is not to be used in the CC evaluated configuration.* - **esp-auth-algorithm** **Syntax:** esp-auth-algorithm {null | md5 | sha1 | sha256 | sha384 | sha512} no esp-auth-algorithm **Context:** config>ipsec>transform **Description**: This command specifies which hashing algorithm should be used for the authentication function Encapsulating Security Payload (ESP). Both ends of a tunnel must share the same configuration parameters in order for the IPSec tunnel to enter the operational state. The null keyword in this command and the null keyword in the esp-encryption-algorithm command are mutually exclusive. The no form of the command returns the parameter to its default value. **Default**: sha1 **Parameters:** null — a very fast algorithm specified in RFC 2410, which provides no authentication md5 — configures ESP to use the hmac-md5 algorithm for authentication sha1 — configures ESP to use the hmac-sha1 algorithm for authentication sha256 — configures ESP to use the sha256 algorithm for authentication sha384 — configures ESP to use the sha384 algorithm for authentication sha512 — configures ESP to use the sha512 algorithm for authentication **Note**: *The null, md5 and sha1 algorithms are not to be used in the CC evaluated configuration.* 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: #**C2023** and #**C2024** Detailed information on the CAVP certificate mapping can be found in the '**section 8 CAVP Mapping**' below.

	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

<table>
<tr><td>Objective</td><td>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.</td></tr>
<tr><td>Evaluator Findings</td><td>The evaluator examined the <b>FCS_COP.1/KeyedHash</b> entry in the section titled <b>TOE Summary Specification</b> in the Security Target 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 states that:

The TOE performs keyed-hash message authentication in accordance with ISO/IEC 9797-2:2011, Section 7 “MAC Algorithm 2”. The details of Key Size and Message Digest Size are given below with the respective HMAC Algorithm.
<table>
<tr><th>HMAC Algorithm</th><th>Hash Function</th><th>Block Size</th><th>Key Lengths</th><th>MAC Lengths</th></tr>
<tr><td>HMAC-SHA-1</td><td>SHA-1</td><td>512 bits</td><td>160 bits</td><td>160 bits</td></tr>
<tr><td>HMAC-SHA-256</td><td>SHA-256</td><td>512 bits</td><td>256 bits</td><td>256 bits</td></tr>
<tr><td>HMAC-SHA-384</td><td>SHA-384</td><td>1024 bits</td><td>384 bits</td><td>384 bits</td></tr>
<tr><td>HMAC-SHA-512</td><td>SHA-512</td><td>1024 bits</td><td>512 bits</td><td>512 bits</td></tr>
</table>
The TOE leverages HMAC algorithm in support of IPSEC and SSH sessions.

Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

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 the sections titled '**SSH**' and '**IPSec**' in the AGD titled '**NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide**' to verify 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. Upon investigation, the evaluator found that the AGD states that:

Message Authentication Code algorithm configuration for SSHv2

- **Configuring SSH MAC Algorithm Lists**

  Use the ssh command to configure SSH2 client and server MAC algorithm lists.
  Client MAC algorithm lists are used if the 7705 SAR is acting as an SSH client, and
  server MAC algorithm lists are used if the 7705 SAR is acting as an SSH server.

  Note: *If a 7705 SAR node is running in FIPS-140-2 mode:*

  - *SSH1 is not supported*
  - *for SSH2, the following MAC algorithms are not available: hmac-sha1-96, hmac-md5, hmac-ripemd160, hmac-ripemd160-openssh-com, and hmac-mda5-96*

- **CLI Syntax:**

```
*A:SR-xx >config>system>security>ssh>server-mac# mac <index> name hmac-sha2-512

*A:SR-xx >config>system>security>ssh>server-mac# mac <index> name hmac-sha2-256

*A:SR-xx >config>system>security>ssh>server-mac# mac <index> name hmac-sha1
```

Internet Key Exchange (IKE) and Transform Commands

- **auth-algorithm**

  Syntax: auth-algorithm {md5 | sha1 | sha256 | sha384 | sha512}
  no auth-algorithm
  Context: config>ipsec>ike-policy
  Description: This command specifies which hashing algorithm to use for the IKE authentication function.
  The no form of the command returns the parameter to its default value.
  Default: sha1

	Parameters: md5 — specifies the hmac-md5 algorithm for authentication sha1 — specifies the hmac-sha1 algorithm for authentication sha256 — specifies the sha256 algorithm for authentication sha384 — specifies the sha384 algorithm for authentication sha512 — specifies the sha512 algorithm for authentication **Note**: *The md5 algorithm is not to be used in the CC evaluated configuration.* 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: #**C2023** and **#C2024** Detailed information on the CAVP certificate mapping can be found in the '**section 8 CAVP Mapping**' below. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8 FCS_RBG_EXT.1

5.2.8.1 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 **FCS_RBG_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that:

	The TOE produces all deterministic random bit generation services in accordance with ISO/IEC 18031:2011 using CTR_DRBG (AES). The TOE uses deterministic RBG, which is seeded by two entropy sources that accumulate entropy. The sources of entropy are from a software-based noise source and a hardware-noise sources. The CTR_DRBG seeded with a minimum of 256 bits of entropy. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.2 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 each AGD and verified that no configuration is required for implementation of the RNG functionality. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.2.8.3 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: #**C2023** and **#C2024** Detailed information on the CAVP certificate mapping can be found in the '**section 8 CAVP Mapping**' below. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3 TSS and Guidance Activities (IPsec)

5.3.1 FCS_IPSEC_EXT.1

5.3.1.1 FCS_IPSEC_EXT.1.1 TSS 1

Objective	The evaluator shall examine the TSS and determine that it describes what takes place when a packet is processed by the TOE, e.g., the algorithm used to process the packet. The TSS describes how the SPD is implemented and the rules for processing both inbound and outbound packets in terms of the IPsec policy. The TSS describes the rules that are available and the resulting actions available after

	matching a rule. The TSS describes how those rules and actions form the SPD in terms of the BYPASS (e.g., no encryption), DISCARD (e.g., drop the packet), and PROTECT (e.g., encrypt the packet) actions defined in RFC 4301.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes what takes place when a packet is processed by the TOE. Upon investigation, the evaluator found that the TSS states that: Incoming packets are inspected against the session database. Sessions that match all the security attributes and do not exceed the TTL are automatically passed on to their destination and are send via a VPN interface where applicable. Packets that do not match the attributes in the session database are then compared to the configured Access Control Lists for that interface identifier and the direction (ingress or egress) based on the ACL entry ID's numerical value. Packets that are permitted are passed to their destination, packets that matches ACLs marked for logging are written to the audit log and packets marked for dropping are discarded. Additionally, the evaluator compared the described rules to the operation of the TOE during testing and found the description of the available SPD to be consistent with the implementation of the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.2 FCS_IPSEC_EXT.1.1 TSS 2

Objective	As noted in section 4.4.1 of RFC 4301, the processing of entries in the SPD is non-trivial and the evaluator shall determine that the description in the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. For example, if the TOE allows specification of ranges, conditional rules, etc., the evaluator shall determine that the description of rule processing (for both inbound and outbound packets) is sufficient to determine the action that will be applied, especially in the case where two different rules may apply. This description shall cover both the initial packets (that is, no SA is established on the interface or for that particular packet) as well as packets that are part of an established SA.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS is sufficient to determine which rules will be applied given the rule structure implemented by the TOE. Upon investigation, the evaluator found that the TSS states that: The TOE permits two actions to be assigned to Access Control Lists – Permit (allow the packet to flow through the TOE with no protection) and Drop (drop the packet with no further processing). The ACLs can be applied to the IPSec VPN tunnels.

	Additionally, the evaluator compared the application of rules within an SPD to the operation of the TOE during testing and found the description of the application of SPD rules to be consistent with the implementation of the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.3 FCS_IPSEC_EXT.1.1 Guidance 1

Objective	The evaluator shall examine the guidance documentation to verify it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. The description includes all three cases – a rule that ensures packets are encrypted/decrypted, dropped, and flow through the TOE without being encrypted. The evaluator shall determine that the description in the guidance documentation is consistent with the description in the TSS, and that the level of detail in the guidance documentation is sufficient to allow the administrator to set up the SPD in an unambiguous fashion. This includes a discussion of how ordering of rules impacts the processing of an IP packet.
Evaluator Findings	The evaluator examined the sections titled **8.1.17 PBR and MFC**, **9.4.9 NGE ACL Interactions** and **7.8.2.1.18 Interface SAP Commands** in the AGD titled **Services Guide** to verify that it instructs the Administrator how to construct entries into the SPD that specify a rule for processing a packet. Upon investigation, the evaluator found that the AGD states that: **8.1.17 PBR and MFC** Both PBR (policy-based routing) and MFC (multi-field classification) are part of the ingress ACL (access control list) configuration on the 7705 SAR. Hence, both PBR and MFC are supported by IPSec on the 7705 SAR, as discussed below: 8.1.17.1 PBR PBR configuration can be applied in two places for an IPSec service. The first place is for VPRN and applies to all incoming access traffic into a private VPRN. In this case, PBR can be used to direct the customer traffic into uplink IPSec tunnels by means of ACL matching criteria. The filtering action of forwarding to an indirect next hop can be used to direct customer traffic into the appropriate IPSec tunnel. The security policy works only on the original (customer packet) IP header; that is, the PBR next hop is not used in making the security policy decision. The second place is for IPSec traffic entering the 7705 SAR from the public domain. A PBR filter can be placed on the network interface, the VPRN interface, or the IES interface to direct the IPSec packet based on the matching/forwarding criteria. In this case, IPSec packets are processed by the PBR filter in the same way as any other IP packet. Note: • All routing decisions are made based on the PBR configuration; therefore, it is possible that even if the packet is destined for the local node security gateway (SeGW), the PBR filter might redirect the packet to another interface.

- Alternatively, for IPSec packets that are not destined for the local node SeGW, PBR can force the packets into the local node SeGW. In this case, the encapsulating security payload (ESP) index of the IPSec packet will not match the SeGW ESP configuration and the packet will be dropped. Thus, it is the responsibility of the network administrator to ensure that the PBR configuration is correct and meets the network needs.

9.4.9 NGE and ACL Interactions

When NGE is enabled on a router interface, the ACL function is applied as follows:

- on ingress — Normal ACLs are applied to traffic received on the interface that could be either NGE-encrypted or clear text. For NGE-encrypted packets, this implies that only the source, destination, and IP options are available to filter on ingress, as the protocol is ESP and the packet is encrypted. If an IP exception ACL is also configured on the interface, the IP exception ACL is applied first to allow any clear text packets to ingress as needed. After the IP exception ACL is applied and if another filter or ACL is configured on the interface, the other filter will process the remaining packet stream (NGE-encrypted and IP exception ACL packets), and other ACL functions such as PBR or Layer 4 information filtering could be applied to any clear text packets that passed the exception ACL.
- on egress — ACLs are applied to packets before they are NGE-encrypted as per normal operation without NGE enabled.

7.8.2.1.18 Interface SAP Commands

egress

Syntax egress

Context config>service>vprn>if>sap

Description This command enables the context to configure egress SAP QoS policies and filter policies. If no sap-egress QoS policy is defined, the system default sap-egress QoS policy is used for egress processing. If no egress filter policy is defined, no filtering is performed.

filter

Syntax filter ip ip-filter-id

no filter ip [ip-filter-id]

filter ipv6 ipv6-filter-id

no filter ipv6 [ipv6-filter-id]

	filter [ip ip-filter-id] [ipv6 ipv6-filter-id] no filter [[ip [ip-filter-id]] [[ipv6 [ipv6-filter-id]] Context config>service>vprn>if>sap>egress config>service>vprn>if>sap>ingress Description This command associates an IPv4 or IPv6 filter policy with an ingress or egress SAP or IP interface. Filter policies control the forwarding and dropping of packets based on IP matching criteria.The filter command is used to associate a filter policy with a specified ip-filter-id or ipv6-filter-id with an ingress or egress SAP. The ip-filter-id or ipv6-filter-id must already be defined before the filter command is executed. If the filter policy does not exist, the operation will fail and an error message will be returned. Only one filter ID can be assigned to an interface unless the interface is dual-stack (supports both IPv4 and IPv6). A dual-stack interface can have one IPv4 and one IPv6 filter ID assigned to it. In general, filters applied to SAPs apply to all packets on the SAP. One exception is that IP match criteria are not applied to non-IP packets, in which case the default action in the filter policy applies to these packets. The no form of this command removes any configured filter ID association with the SAP or IP interface. The filter ID is not removed from the system unless the scope of the created filter is set to local. To avoid deletion of the filter ID and only break the association with the service object, use the scope command within the filter definition to change the scope to local or global. The default scope of a filter is local. Parameters ip-filter-id — the IPv4 filter policy. The filter ID or filter name must already exist within the created IPv4 filters. Values 1 to 65535 or filter-name (up to 64 characters) Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.4 FCS_IPSEC_EXT.1.3 TSS 1

Objective	The evaluator checks the TSS to ensure it states that the VPN can be established to operate in transport mode and/or tunnel mode (as identified in FCS_IPSEC_EXT.1.3).
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS states that the VPN can be established to operate in transport mode and/or tunnel mode (as identified in FCS_IPSEC_EXT.1.3). Upon investigation, the evaluator found that the TSS states that: The TOE implements IPSec in accordance with RFC 4301 in tunnel mode only. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.5 FCS_IPSEC_EXT.1.3 Guidance 1

Objective	The evaluator shall confirm that the guidance documentation contains instructions on how to configure the connection in each mode selected.
Evaluator Findings	The evaluator examined the sections titled **8.7.4 Configuring IPSec and IPSec Tunnels in Services** in the AGD titled **Services Guide** to verify that it contains instructions on how to configure the connection in each mode selected. Upon investigation, the evaluator found that the AGD states that: **8.7.4 Configuring IPSec and IPSec Tunnels in Services** IPSec is configured under IES and VPRN services. For the private-side IPSec tunnel interface and SAP, under the VPRN service context, configure IPSec security policies, and create tunnel interfaces, private tunnel SAPs, IPSec tunnels, and IPSec tunnel parameters. The tunnel keyword must be used when creating an interface for a private tunnel SAP. For a public-side IPSec tunnel interface and SAP, under the IES or VPRN service context, create an interface and public tunnel SAP. The tunnel keyword is not used when creating an interface for a public tunnel SAP. Private-side and public-side tunnels function in pairs, where a pair is defined by the service ID and the interface subnet. The local gateway address and delivery service configured using the VPRN ipsec-tunnel>local-gateway-address command correspond to the IES or VPRN interface address and service ID where the public-side tunnel interface is defined. In the example below, the local-gateway-address is 10.10.10.11 and the delivery-service is 10.

The following example displays the configuration output when configuring IPSec for a private-side VPRN service and a public-side IES.

```
*A:7705custDoc:Sar18>config>service>vprn# info detail
----------------------------------------------
...
ipsec
security-policy 1 create
entry 1 create
local-ip any
remote-ip any
exit
entry 2 create
local-ip 198.51.100.0/24
remote-ip 198.51.100.0/24
exit
exit
security-policy 15 create
entry 15 create
no local-ip
no remote-ip
exit
exit
exit
...
```

	interface "vprn_tunnel" tunnel create no ip-mtu sap tunnel-1.private:22 create no description ingress qos 1 exit egress qos 1 no filter no agg-rate-limit exit ipsec-tunnel "ipsec_tunnel_tag1" create shutdown no description security-policy 1 2 local-gateway address 10.10.10.11 peer 10.10.10.11 delivery-service 10 no bfd-designate no clear-df-bit no ip-mtu exit no shutdown exit

```
no shutdown
exit
no service-name
static-route-entry 192.100.200.10/32
ipsec-tunnel "ipsec_tunnel_tag1"
no shutdown
exit
exit
---------------------------------------------
```

The same information about configuring the IPSec tunnel can be found in the section **‘IPSec’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** In addition, this CC guide also states the following additional clarification:

1. Configuring IPSec and IPSec Tunnels in Services

- IPSec is configured under VPRN services. The device operates only in tunnel mode by default and no separate configuration is required. For the private-side IPSec tunnel interface and SAP, under the VPRN service context, configure IPSec security policies, and create tunnel interfaces, private tunnel SAPs, IPSec tunnels, and IPSec tunnel parameters. The tunnel keyword must be used when creating an interface for a private tunnel SAP.
- For a public-side IPSec tunnel interface and SAP, under VPRN service context, create an interface and public tunnel SAP. The tunnel keyword is not used when creating an interface for a public tunnel SAP.
- Private-side and public-side tunnels function in pairs, where a pair is defined by the service ID and the interface subnet.
- The local gateway address and delivery service configured using the VPRN ipsec-tunnel>local-gateway-address command correspond to the VPRN interface address and service ID where the public-side tunnel interface is defined. In the example below, the local-gateway-address is 10.1.5.28 and the delivery-service is 3.

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

Verdict	Pass

5.3.1.6 FCS_IPSEC_EXT.1.4 TSS 1

Objective	The evaluator shall examine the TSS to verify that the selected algorithms are implemented. In addition, the evaluator ensures that the SHA-based HMAC algorithm conforms to the algorithms specified in FCS_COP.1/KeyedHash Cryptographic Operations (for keyed-hash message authentication) and if the SHA-based HMAC function truncated output is utilized it must also be described.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS states that the selected algorithms are implemented. Upon investigation, the evaluator found that the TSS states that: The TOE implements IPSec in accordance with RFC 4301 in tunnel mode only. The TOE implements AES-CBC-128, AES-CBC-192 and AES-CBC-256 using HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-256 for ESP protection. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.1.7 FCS_IPSEC_EXT.1.4 Guidance 1

Objective	The evaluator checks the guidance documentation to ensure it provides instructions on how to configure the TOE to use the algorithms selected.
Evaluator Findings	The evaluator examined the section titled **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** in the AGD titled **Services Guide** to verify that it provides instructions on how to configure the TOE to use the algorithms selected. Upon investigation, the evaluator found that the AGD states that: auth-algorithm Syntax auth-algorithm {md5 | sha1 | sha256 | sha384 | sha512} no auth-algorithm Context config>ipsec>ike-policy Description This command specifies which hashing algorithm to use for the IKE authentication function. The no form of the command returns the parameter to its default value. Default sha1 Parameters md5 — specifies the hmac-md5 algorithm for authentication sha1 — specifies the hmac-sha1 algorithm for authentication

sha256 — specifies the sha256 algorithm for authentication

sha384 — specifies the sha384 algorithm for authentication

sha512 — specifies the sha512 algorithm for authentication

encryption-algorithm

Syntax encryption-algorithm {des | 3des | aes128 | aes192 | aes256}

no encryption-algorithm

Context config>ipsec>ike-policy

Description This command specifies the encryption algorithm to use for the IKE session.

The no form of the command returns the algorithm to its default value (aes128).

Default aes128

Parameters des — configures the 56-bit des algorithm for encryption. This is an older algorithm, with
relatively weak security. It should only be used when a strong algorithm is not
available at both ends at an acceptable performance level.

3des — configures the 3-des algorithm for encryption. This is a modified application of
the des algorithm that uses multiple des operations for more security.

aes128 — configures the aes algorithm with a block size of 128 bits. This is the
mandatory implementation size for aes.

esp-auth-algorithm

Syntax esp-auth-algorithm {null | md5 | sha1 | sha256 | sha384 | sha512}

no esp-auth-algorithm

Context config>ipsec>transform

Description This command specifies which hashing algorithm should be used for the authentication

	function Encapsulating Security Payload (ESP). Both ends of a tunnel must share the same configuration parameters in order for the IPSec tunnel to enter the operational state. The null keyword in this command and the null keyword in the esp-encryption-algorithm command are mutually exclusive. The no form of the command returns the parameter to its default value. Default sha1 Parameters null — a very fast algorithm specified in RFC 2410, which provides no authentication md5 — configures ESP to use the hmac-md5 algorithm for authentication sha1 — configures ESP to use the hmac-sha1 algorithm for authentication sha256 — configures ESP to use the sha256 algorithm for authentication sha384 — configures ESP to use the sha384 algorithm for authentication sha512 — configures ESP to use the sha512 algorithm for authentication esp-encryption-algorithm Syntax esp-encryption-algorithm {null | des | 3des | aes128 | aes192 | aes256} no esp-encryption-algorithm Context config>ipsec>transform Description This command specifies the encryption algorithm to use for the IPSec session. Encryption only applies to Encapsulating Security Payload (ESP) configurations. For IPSec tunnels to come up, both ends of the IPSec tunnel (both private-side endpoints) must be configured with the same encryption algorithm. That is, the configuration for vprn>if>sap> ipsec-tunnel transform must match at both nodes. The null keyword in this command and the null keyword in the esp-auth-algorithm command are mutually exclusive.

The no form of the command returns the parameter to its default value.

Default aes128

Parameters null — configures the high-speed null algorithm, which does nothing. This is the same as not having encryption turned on.

des — configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. Although slightly better than no encryption, it should only be used when a strong algorithm is not available at both ends at an acceptable performance level.

3des — configures the 3-des algorithm for encryption. This is a modified application of the des algorithm that uses multiple des operations to make things more secure.

aes128 — configures the aes algorithm with a block size of 128 bits. This is the mandatory implementation size for aes. This is a very strong algorithm choice.

aes192 — configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes.

aes256 — configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes.

The same information about configuring the IPSec tunnel can be found in the section **'IPSec'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow:

5.3.2 **Internet Key Exchange (IKE) and Transform Commands**

- **auth-algorithm**
  Note: *The md5 algorithm is not to be used in the CC evaluated configuration.*
- **dh-group**
  Note: *The DH Groups (1, 2, 5) should not be used in the CC evaluated configuration.*
- **encryption-algorithm**

	Note: *The des, and 3des algorithms are not to be used in the CC evaluated configuration.* - **esp-auth-algorithm** **Note**: *The null, md5 and sha1 algorithms are not to be used in the CC evaluated configuration.* - **esp-encryption-algorithm** **Note**: *The null, des, and 3des algorithms are not to be used in the CC evaluated configuration.* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.1 FCS_IPSEC_EXT.1.5 TSS 1

Objective	The evaluator shall examine the TSS to verify that IKEv1 and/or IKEv2 are implemented.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies whether IKEv1 and/or IKEv2 are implemented. Upon investigation, the evaluator found that the TSS states that: Both IKEv1 and IKEv2 are implemented. IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109 and RFC 4868 for hash functions; IKEv2 as defined in RFCs 5996 (with support for NAT traversal) and RFC 4868 for hash functions. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.2 FCS_IPSEC_EXT.1.5 TSS 2

Objective	For IKEv1 implementations, the evaluator shall examine the TSS to ensure that, in the description of the IPsec protocol, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. It may be that this is a configurable option.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used. Upon investigation, the evaluator found that the TSS states that: Both IKEv1 and IKEv2 are implemented. IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109 and RFC 4868 for hash functions; IKEv2 as defined in RFCs 5996 (with support for NAT traversal) and RFC 4868 for hash functions. IKEv1 aggressive mode is not supported, and only main mode is permitted in the evaluated configuration. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.3.2.3 FCS_IPSEC_EXT.1.5. Guidance 1

Objective	The evaluator shall check the guidance documentation to ensure it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and how to configure the TOE to perform NAT traversal (if selected).
Evaluator Findings	The evaluator examined the section titled **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** in the AGD titled **Services Guide** to verify that it instructs the administrator how to configure the TOE to use IKEv1 and/or IKEv2 (as selected), and how to configure the TOE to perform NAT traversal (if selected). Upon investigation, the evaluator found that the AGD states that: **ike-version** Syntax ike-version {1 | 2} no ike-version Context config>ipsec>ike-policy Description This command configures the version of the IKE protocol that the IKE policy will use. The no form of the command removes the configured version. Default 2 Parameters 1 — specifies that the IKE policy will use IKEv1 2 — specifies that the IKE policy will use IKEv2 **nat-traversal** Syntax nat-traversal [force] [keep-alive-interval keep-alive-interval] [force-keep-alive] no nat-traversal Context config>ipsec>ike-policy Description This command specifies whether NAT-T (Network Address Translation Traversal) is enabled, disabled, or in force mode. Enabling NAT-T enables the NAT detection mechanism. If a NAT device is detected in the path between the 7705 SAR and its IPSec peer, then UDP encapsulation is done on the IPSec packet to allow the IPSec traffic to traverse the NAT

	device. When nat-traversal is used without any parameters, NAT-T is enabled and sending keepalive packets is disabled (keep-alive-interval is 0 s). When the force keyword is used, the IPSec tunnel always uses a UDP value in its header, regardless of whether a NAT device is detected. The force-keep-alive keyword specifies whether keepalive packets are sent only when a NAT device is detected or are always sent (regardless of detection of a NAT device). When force-keep-alive is used, packets are always sent and the “Behind NAT Only” field in the show>ipsec>ike-policy ike-policy-id indicates False. When force-keep-alive is not used, packets are may or may not be sent, depending on the whether NAT-T is enabled or disabled. In this case, the “Behind NAT Only” field indicates True. The keep-alive-timer keyword defines the frequency, where “0” means that keepalives are disabled. The no form of the command returns the parameters to the default values (NAT-T is disabled, keep-alive-interval is 0 s, and force-keep-alive is True). Default no nat-traversal Parameters force — when specified, forces NAT-T to be enabled keep-alive-interval — specifies the keepalive interval for NAT-T. If the value is 0 s, then keepalive messages are disabled. Values 120 to 600 s Default 0 s force-keep-alive — specifies that NAT-T keepalive packets are always sent, regardless of NAT detection results Based on these findings, this assurance activity is considered satisfied.

	The same information about configuring the IPSec tunnel can be found in the section **'IPSec'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.**
Verdict	Pass

5.3.2.4 FCS_IPSEC_EXT.1.5. Guidance 2

Objective	If the IKEv1 Phase 1 mode requires configuration of the TOE prior to its operation, the evaluator shall check the guidance documentation to ensure that instructions for this configuration are contained within that guidance.
Evaluator Findings	The evaluator examined the section titled **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** in the AGD titled **Services Guide** to verify that it contains any necessary instructions for IKEv1 Phase 1 mode configuration. Upon investigation, the evaluator found that the AGD states that: ike-mode Syntax ike-mode {main | aggressive} no ike-mode Context config>ipsec>ike-policy Description This command specifies the mode of operation for IKEv1 phase 1, either main mode or aggressive mode. The difference between the modes is the number of messages used to establish the session. IKEv1 phase 1 main mode uses three pairs of messages (for a total of six messages) between IPSec peers. IKEv1 phase 1 aggressive mode has only three message exchanges. This command does not apply to IKEv2. The no form of the command removes the mode of operation. Default main Parameters main — specifies that IKEv1 phase 1 will operate in main mode aggressive — specifies that IKEv1 phase 1 will operate in aggressive mode.

	The same information about configuring the IPSec tunnel can be found in the section **'IPSec'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.5 FCS_IPSEC_EXT.1.6 TSS 1

Objective	The evaluator shall ensure the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms chosen in the selection of the requirement are included in the TSS discussion.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the algorithms used for encrypting the IKEv1 and/or IKEv2 payload, and that the algorithms chosen in the selection of the requirement are included in the TSS discussion. Upon investigation, the evaluator found that the TSS states that: The TOE implements AES-CBC-128, AES-CBC-192 and AES-CBC-256 for payload protection in IKEv1 and IKEv2. The TOE uses HMAC DRBG with SHA-1, SHA-256, SHA-384 and SHA-512 for the generation of DH exponents and nonces. Nonces in the IKE key exchange protocol are always of length 256 bits, whether for DH Group 14 or DH Group 15 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.2.6 FCS_IPSEC_EXT.1.6 Guidance 1

Objective	The evaluator ensures that the guidance documentation describes the configuration of all selected algorithms in the requirement.
Evaluator Findings	The evaluator examined the section titled **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** in the AGD titled **Services Guide** to verify that it describes the configuration of all selected algorithms in the requirement. Upon investigation, the evaluator found that the AGD states that: encryption-algorithm Syntax encryption-algorithm {des | 3des | aes128 | aes192 | aes256} no encryption-algorithm Context config>ipsec>ike-policy

	Description This command specifies the encryption algorithm to use for the IKE session. The no form of the command returns the algorithm to its default value (aes128). Default aes128 Parameters des — configures the 56-bit des algorithm for encryption. This is an older algorithm, with relatively weak security. It should only be used when a strong algorithm is not available at both ends at an acceptable performance level. 3des — configures the 3-des algorithm for encryption. This is a modified application of the des algorithm that uses multiple des operations for more security. aes128 — configures the aes algorithm with a block size of 128 bits. This is the mandatory implementation size for aes. aes192 — configures the aes algorithm with a block size of 192 bits. This is a stronger version of aes. aes256 — configures the aes algorithm with a block size of 256 bits. This is the strongest available version of aes. esp-encryption-algorithm Syntax esp-encryption-algorithm {null | des | 3des | aes128 | aes192 | aes256} no esp-encryption-algorithm Context config>ipsec>transform Description This command specifies the encryption algorithm to use for the IPSec session. Encryption only applies to Encapsulating Security Payload (ESP) configurations. For IPSec tunnels to come up, both ends of the IPSec tunnel (both private-side endpoints) must be configured with the same encryption algorithm. That is, the configuration for vprn>if>sap> ipsec-tunnel transform must match at both nodes.

The null keyword in this command and the null keyword in the esp-auth-algorithm

command are mutually exclusive.

The no form of the command returns the parameter to its default value.

Default aes128

Parameters null — configures the high-speed null algorithm, which does nothing. This is the same as

not having encryption turned on.

des — configures the 56-bit des algorithm for encryption. This is an older algorithm, with

relatively weak security. Although slightly better than no encryption, it should only be

used when a strong algorithm is not available at both ends at an acceptable

performance level.

3des — configures the 3-des algorithm for encryption. This is a modified application of

the des algorithm that uses multiple des operations to make things more secure.

aes128 — configures the aes algorithm with a block size of 128 bits. This is the

mandatory implementation size for aes. This is a very strong algorithm choice.

aes192 — configures the aes algorithm with a block size of 192 bits. This is a stronger

version of aes.

aes256 — configures the aes algorithm with a block size of 256 bits. This is the strongest

available version of aes.

The same information about configuring the IPSec tunnel can be found in the section **‘IPSec’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow:

5.3.3 Internet Key Exchange (IKE) and Transform Commands

- **auth-algorithm**

	Note: *The md5 algorithm is not to be used in the CC evaluated configuration.* - **dh-group** **Note**: *The DH Groups (1, 2, 5) should not be used in the CC evaluated configuration.* - **encryption-algorithm** **Note:** *The des, and 3des algorithms are not to be used in the CC evaluated configuration.* - **esp-auth-algorithm** **Note**: *The null, md5 and sha1 algorithms are not to be used in the CC evaluated configuration.* - **esp-encryption-algorithm** **Note**: *The null, des, and 3des algorithms are not to be used in the CC evaluated configuration.* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.1 FCS_IPSEC_EXT.1.7 TSS 1

Objective	The evaluator shall ensure the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 1 SA lifetime and/or the IKEv2 SA lifetime. The evaluator shall verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 1 SA lifetime and/or the IKEv2 SA lifetime and that information corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the TSS states that: In the evaluated configuration, the TOE permits configuration of the: - IKEv1 Phase 1 and IKEv2 SA lifetimes in terms of length of time (1,200 to 172,800 seconds), The lifetime of the IPsec SA is configured through the CLI only accessible to the administrators of the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.2 FCS_IPSEC_EXT.1.7 Guidance 1 **[TD0633]**

Objective	The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the Guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 24 hours is exceeded (e.g. configure a time value of 23h 45min to ensure the actual rekey is

	performed no later than 24h). The evaluator shall verify that the Guidance documentation allows the Administrator to configure the Phase 1 SA value of 24 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 24 hours. It is not permitted to configure a value of 24 hours if that leads to an actual rekey after more than 24hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.
Evaluator Findings	The evaluator examined the section titled **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** in the AGD titled **Services Guide** to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD states that: isakmp-lifetime Syntax isakmp-lifetime isakmp-lifetime no isakmp-lifetime Context config>ipsec>ike-policy Description This command specifies the lifetime of a phase 1 SA. ISAKMP stands for Internet Security Association and Key Management Protocol. The no form of the command returns the isakmp-lifetime value to the default value. Default 86400 Parameters isakmp-lifetime — specifies the lifetime of the phase 1 IKE key, in seconds Values 1200 to 172800 The same information about configuring the IPSec tunnel can be found in the section **'IPSec'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.3 FCS_IPSEC_EXT.1.8 TSS 1

Objective	The evaluator shall ensure the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 2 SA lifetime and/or the IKEv2 Child SA lifetime. The evaluator shall verify that the selection made here corresponds to the selection in FCS_IPSEC_EXT.1.5.

Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies the lifetime configuration method used for limiting the IKEv1 Phase 2 SA lifetime and/or the IKEv2 Child SA lifetime and that the information corresponds to the selection in FCS_IPSEC_EXT.1.5. Upon investigation, the evaluator found that the TSS states that**:** In the evaluated configuration, the TOE permits configuration of the: • IKEv1 Phase 2 SA and IKEv2 Child SA lifetimes in terms of length of time (1,200 to 172,800 seconds) The lifetime of the IPsec SA is configured through the CLI only accessible to the administrators of the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.4 FCS_IPSEC_EXT.1.8 Guidance 1 **[TD0633]**

Objective	The evaluator shall verify that the values for SA lifetimes can be configured and that the instructions for doing so are located in the Guidance documentation. If time-based limits are supported, configuring the limit may lead to a rekey no later than the specified limit. For some implementations, it may be necessary, though, to configure the TOE with a lower time value to ensure a rekey is performed before the maximum SA lifetime of 8 hours is exceeded (e.g. configure a time value of 7h 45min to ensure the actual rekey is performed no later than 8h). The evaluator shall verify that the Guidance documentation allows the Administrator to configure the Phase 2 SA value of 8 hours or provides sufficient instruction about the time value to configure to ensure the rekey is performed no later than the maximum SA lifetime of 8 hours. It is not permitted to configure a value of 8 hours if that leads to an actual rekey after more than 8hours. Currently there are no values mandated for the number of bytes, the evaluator just ensures that this can be configured if selected in the requirement.
Evaluator Findings	The evaluator examined the section titled **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** in the AGD titled **Services Guide** to verify that it includes instructions for configuring values for SA lifetimes. Upon investigation, the evaluator found that the AGD states that: ipsec-lifetime Syntax ipsec-lifetime ipsec-lifetime no ipsec-lifetime Context config>ipsec>ike-policy Description This parameter specifies the lifetime of a phase 2 SA. The no form of the command returns the ipsec-lifetime value to the default.

	Default 3600 (1 hr) Parameters ipsec-lifetime — specifies the lifetime of the phase 2 IKE key, in seconds Values 1200 to 172800 The same information about configuring the IPSec tunnel can be found in the section **‘IPSec’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.5 FCS_IPSEC_EXT.1.9 TSS 1

Objective	The evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating "x". The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of "x" meets the stipulations in the requirement.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the process for generating "x" for each DH group supported. Upon investigation, the evaluator found that the TSS states that: The TOE utilizes CTR-DRBG with AES (as specified in FCS_RBG_EXT.1) to generate the exponents used in IKE key exchanges, having the possible lengths of 224 or 256 bits, corresponding to each of the supported DH groups. For Diffie-Hellman Groups 14 and 15 the TOE always generates value x of 256 bits. For DH Group 14 only 224 of those bits are used. For DH Group 15 all 256 bits are used. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.6 FCS_IPSEC_EXT.1.10 TSS 1

Objective	If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.

	If the second selection is chosen, the evaluator shall check to ensure that, for each PRF hash supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the process for generating each nonce for each DH group or PRF hash supported and indicates that the random number generated that meets the requirements in this PP is used, and indicates that the length of the nonces meet the stipulations in the requirement. Upon investigation, the evaluator found that the TSS states that: The TOE uses HMAC DRBG with SHA-1, SHA-256, SHA-384 and SHA-512 for the generation of DH exponents and nonces. Nonces in the IKE key exchange protocol are always of length 256 bits, whether for DH Group 14 or DH Group 15. The generation of random bits is described at FCS_RBG_EXT.1. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.7 FCS_IPSEC_EXT.1.11 TSS 1

Objective	The evaluator shall check to ensure that the DH groups specified in the requirement are listed as being supported in the TSS. If there is more than one DH group supported, the evaluator checks to ensure the TSS describes how a particular DH group is specified/negotiated with a peer.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists the DH groups specified in the requirement as being supported. Upon investigation, the evaluator found that the TSS states that: The TOE implements Diffie-Hellman Groups 14 and 15. In the IKEv1 phase 1 and phase 2 exchanges, the TOE and peer will agree on the best DH group both can support. When the TOE receives an IKE proposal, it will select the first DH group that matches the acceptable DH groups. The negotiation will fail if there is no match. Similarly, when the peer initiates the IKE protocol, the TOE will select the first match from the IKE proposal sent by the peer and the negotiation fails is no acceptable match is found. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.3.8 FCS_IPSEC_EXT.1.11 Guidance 1

Objective	The evaluator ensures that the guidance documentation describes the configuration of all algorithms selected in the requirement.
Evaluator Findings	The evaluator examined the section titled **8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands** in the AGD titled **Services Guide** to verify that it describes the configuration of all algorithms selected in the requirement. Upon investigation, the evaluator found that the AGD states that: dh-group Syntax dh-group {1 | 2 | 5 | 14 | 15} no dh-group Context config>ipsec>ike-policy Description This command specifies which Diffie-Hellman group is used to calculate session keys: • Group1: 768 bits • Group2: 1024 bits • Group5: 1536 bits • Group14: 2048 bits • Group15: 3072 bits More bits provide a higher level of security but require more processing. The no form of the command returns the parameter to its default value (Group2). Default no dh-group (Group2) The same information about configuring the IPSec tunnel can be found in the section **'IPSec'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow: ***5.3.4* Internet Key Exchange (IKE) and Transform Commands** • **auth-algorithm** **Note**: *The md5 algorithm is not to be used in the CC evaluated configuration.* • **dh-group**

	Note: *The DH Groups (1, 2, 5) should not be used in the CC evaluated configuration.* • **encryption-algorithm** **Note:** *The des, and 3des algorithms are not to be used in the CC evaluated configuration.* • **esp-auth-algorithm** **Note**: *The null, md5 and sha1 algorithms are not to be used in the CC evaluated configuration.* • **esp-encryption-algorithm** **Note**: *The null, des, and 3des algorithms are not to be used in the CC evaluated configuration.* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.1 FCS_IPSEC_EXT.1.12 TSS 1

Objective	The evaluator shall check that the TSS describes the potential strengths (in terms of the number of bits in the symmetric key) of the algorithms that are allowed for the IKE and ESP exchanges. The TSS shall also describe the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites to ensure that the strength (in terms of the number of bits of key in the symmetric algorithm) of the negotiated algorithm is less than or equal to that of the IKE SA this is protecting the negotiation.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes the potential strengths of the algorithms that are allowed for the IKE and ESP exchanges and the checks that are done when negotiating IKEv1 Phase 2 and/or IKEv2 CHILD_SA suites. Upon investigation, the evaluator found that the TSS states that: The TOE checks the strengths of the configured IKE algorithms prior to committing a tunnel configuration. This ensures that the strength of the symmetric algorithm (128, 192 or 256 bits) negotiated to protect the IKEv1 Phase 1 or IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm negotiated to protect the IKEv1 Phase 2 or IKEv2 CHILD_SA connection. If the strength is not greater, an error is displayed, and the configuration fails. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.2 FCS_IPSEC_EXT.1.13 TSS 1

Objective	The evaluator ensures that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication. The description must be consistent with the algorithms as specified in FCS_COP.1/SigGen Cryptographic Operations (for cryptographic signature).

Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies RSA and/or ECDSA as being used to perform peer authentication and that the algorithms are consistent with those specified in FCS_COP.1/SigGen Cryptographic Operations. Upon investigation, the evaluator found that the TSS states that: The TOE permits peer authentication via RSA that use X.509v3 certificates that conform to RFC 4945 or pre-shared keys. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.3 FCS_IPSEC_EXT.1.13 TSS 2

Objective	If pre-shared keys are chosen in the selection, the evaluator shall check to ensure that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. The description in the TSS shall also indicate how pre-shared key establishment is accomplished for TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how pre-shared keys are established and used in authentication of IPsec connections. Upon investigation, the evaluator found that the TSS states that: The TOE accepts bit-based pre-shared keys. The TOE converts text-based pre-shared keys into an authentication value as per RFC 2409 for IKEv1 or RFC 4306 for IKEv2, using SHA-1 or the PRF that is configured as the hash algorithm for the IKE exchanges. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.4 FCS_IPSEC_EXT.1.13 Guidance 1

Objective	The evaluator ensures the guidance documentation describes how to set up the TOE to use certificates with RSA and/or ECDSA signatures and public keys.
Evaluator Findings	The evaluator examined the section titled **8.10.1.2.1 X.509 and Certificate Commands** in the AGD titled **Services Guide** to verify that it describes how to set up the TOE to use certificates with RSA and/or ECDSA signatures and public keys. Upon investigation, the evaluator found that the AGD states that: gen-keypair

	Syntax gen-keypair url-string [size {512 | 1024 | 2048}] [type {rsa | dsa}] Context admin>certificate Description This command generates an RSA or DSA private key/public key pair and stores it in a local file in the cf3:\system-pki\key directory. Parameters url-string — the name of the key file Values url-string : local-url, 99 characters maximum local-url : cflash-id/file-path cflash-id : cf1:, cf2:, cf3: size — the key size in bits (the minimum key size is 1024 bits when running in FIPS-140- 2 mode) Values 512, 1024, or 2048 Default 2048 type — the type of key Values rsa, dsa Default rsa The same information about configuring the x509 certificates can be found in the section **‘X509 Certificates’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow: **Note:** *The key sizes 512 and 1024 are not supported in FIPS mode. The DSA key pairs should not be configured in the CC evaluated configuration. The minimum key size is 2048 bits in FIPS mode.* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.5 FCS_IPSEC_EXT.1.13 Guidance 2

Objective	The evaluator shall check that the guidance documentation describes how preshared keys are to be generated and established. The description in the guidance documentation shall also indicate how pre-shared key establishment is accomplished for TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.
Evaluator Findings	The evaluator examined the section titled **8.10.2.2.3 IPSec PKI Commands** in the AGD titled **Services Guide** to verify that it describes how pre-shared keys are to be generated and established. Upon investigation, the evaluator found that the AGD states that: auth-method Syntax auth-method {psk | cert-auth} no auth-method Context config>ipsec>ike-policy Description This command specifies the authentication method used with this IKE policy. The no form of the command removes the parameter from the configuration. Default no auth-method own-auth-method Syntax own-auth-method {psk | cert} no own-auth-method Context config>ipsec>ike-policy Description This command configures the authentication method used with this IKE policy on its own side. The same information about configuring the IPSec tunnel can be found in the section **‘IPSec’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.6 FCS_IPSEC_EXT.1.13 Guidance 3

Objective	The evaluator will ensure that the guidance documentation describes how to configure the TOE to connect to a trusted CA and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”.
Evaluator Findings	The evaluator examined the sections titled **8.1.2 X.509v3 Certificate Overview, 8.1.2.2 Local Storage, 8.1.2.3 CA Profile, 8.1.4 Trust Anchor Profile** and **8.10.2.3 Show Commands** in the AGD titled **Services Guide** to verify that it describes how to configure the TOE to connect to a trusted CA and ensure a valid certificate for that CA is loaded into the TOE and marked “trusted”. Upon investigation, the evaluator found that the AGD states that: **8.1.2.2 Local Storage** The 7705 SAR requires the following objects to be stored locally as a file: • CA certificate • CRL • the system’s own certificate • the system’s own key All these objects must be imported with the admin certificate import command before they can be used by the 7705 SAR. The import process converts the format of the input file to distinguished encoding rules (DER), encrypts the key file, and saves it in the cf3:/system-pki directory. **8.1.2.3 CA Profile** On the 7705 SAR, the CA-related configuration is stored in a CA profile that contains the following configurable items: • name and description • CA’s certificate — an imported certificate • CA’s CRL— an imported CRL • revocation check method — specifies the way the CA checks the revocation

	status of the certificate it issued • CMPv2 — a CMPv2 server-related configuration • OCSP— an OCSP responder-related configuration When a user enables a ca-profile (no shutdown), the system loads the specified CA certificate and CRL into memory. The following checks are performed: • for the CA certificate: - all mandatory fields defined in section 4.1 of RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, exist and conform to the RFC 5280 defined format - the version field value is 0x2 - the validity field indicates that the certificate is still in its validity period - the X.509 Basic Constraints extension exists and the CA Boolean value is true - if the Key Usage extension exists, at the least), the keyCertSign and cRLSign are asserted **8.10.2.3 Show Commands** trust-anchor-profile Syntax trust-anchor-profile name [create] no trust-anchor-profile name Context config>ipsec Description This command specifies the trust-anchor-profile for the IPSec tunnel. This command will override the trust-anchor-profile configuration in the config>service>vprn>if>sap>ipsectunnel>cert context. Default no trust-anchor-profile Parameters profile-name — the trust-anchor-profile name

	The same information about configuring the x509 certificates can be found in the section **'X509 Certificates'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.**
Verdict	Pass

5.3.4.7 FCS_IPSEC_EXT.1.14 TSS 1

Objective	The evaluator shall ensure that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. This description shall include which field(s) of the certificate are used as the presented identifier (DN, Common Name, or SAN). If the TOE simultaneously supports the same identifier type in the CN and SAN, the TSS shall describe how the TOE prioritizes the comparisons (e.g. the result of comparison if CN matches but SAN does not). If the location (e.g. CN or SAN) of non-DN identifier types must explicitly be configured as part of the reference identifier, the TSS shall state this. If the ST author assigned an additional identifier type, the TSS description shall also include a description of that type and the method by which that type is compared to the peer's presented certificate, including what field(s) are compared and which fields take precedence in the comparison.
Evaluator Findings	The evaluator examined the **FCS_IPSEC_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how the TOE compares the peer's presented identifier to the reference identifier. Upon investigation, the evaluator found that the TSS states that: When using certificates for peer authentication, the TOE will only establish a trusted channel to peers that provide a valid certificate. The TOE will compare the reference identifier of the peer against the reference identifier stored in the associated certificate. If the two values are not a match, the TOE will not establish the connection. The TOE supports SAN:IP addresses, SAN:FQDNs, and SAN:User FQDN (email address) reference identifiers. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.3.4.8 FCS_IPSEC_EXT.1.14 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 does not guarantee unique identifiers, 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 the section titled ‘**IPSec’,** sub-section **‘Configuring Reference Identifiers’** in the AGD titled ‘**NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’** to verify that it 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). Upon investigation, the evaluator found that the AGD states that: **2. Configuring Reference Identifiers** • The TOE supports the following reference identifiers: ○ SAN: IP address ○ SAN: FullyQualifiedDomainName (FQDN) ○ SAN: user FQDN • The following configuration is used to configure reference identifiers on the device: `remote-id type <ipv4, fqdn, email> value` *`value`* 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 **[TD0631]**

Objective	The evaluator shall check to ensure that the TSS contains a list of supported public key algorithms that are accepted for client authentication and that this list is consistent with signature verification algorithms selected in FCS_COP.1/SigGen (e.g., accepting EC keys requires corresponding Elliptic Curve Digital Signature algorithm claims). 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. If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, then the evaluator shall confirm its role in the authentication process is described in the TSS.

Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, 4256, 4344, 6668, 8268, 8308 (Section 3.1) and 8332. 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 **FCS_SSHS_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE ensures that packets greater than 65000 bytes in an SSH transport connection are dropped as described in RFC 4253. 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 **FCS_SSHS_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS specifies the optional characteristics and the encryption algorithms supported. Upon investigation, the evaluator found that the TSS states that: The TOE supports the following encryption algorithms: aes128-cbc, aes256-cbc aes128-ctr, and aes256-ctr for SSH transport. 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 the section titled **3.10.2.1.13 SSH Commands** in the AGD titled **System Management Guide** 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 states that: 3.10.2.1.13 SSH Commands ssh Syntax ssh Context config>system>security Description This command enables the context to configure the SSH server parameters on the system. Quitting SSH while in the process of authentication is accomplished by either executing a ctrl-c or "~." (tilde and dot), assuming the "~" is the default escape character for the SSH session. cipher Syntax cipher index name cipher-name no cipher index Context config>system>security>ssh>client-cipher-list config>system>security>ssh>server-cipher-list Description This command configures the allowed SSH protocol version 1 or version 2 ciphers that are available on the SSH client or server. Client cipher and server cipher lists are used to negotiate the best compatible cipher between the SSH client and SSH server. Client ciphers are used when the 7705 SAR node is acting as an SSH client; server ciphers are used when the 7705 SAR node is acting as an SSH server.

	Values For SSHv2: client ciphers: aes128-ctr, aes192-ctr, aes256-ctr, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc server ciphers: aes128-ctr, aes192-ctr, aes256-ctr, 3des-cbc, blowfish-cbc, cast128-cbc, arcfour, aes128-cbc, aes192-cbc, aes256-cbc, rijndael-cbc The same information about the SSH protocol can be found in the section **'SSH'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow: **Note**: • *The blowfish-cbc, cast128-cbc, arcfour, and rijndael-cbc ciphers are not available if the 7705 SAR node is running in FIPS-140-2 mode.* • *The cryptographic keys - aes192-ctr and aes192-cbc are not to be used in the CC evaluated configuration because these two algorithms are not allowed for SSH in NDcPP 2.2e.* • *The protocol-version 1 is not available under FIPS-140-2 mode.* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.4.1.5 FCS_SSHS_EXT.1.5 TSS 1 **[TD0631]**

Objective	The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that the SSH server's host public key algorithms supported are specified and that they are identical to those listed for this component.

Evaluator Findings	The evaluator examined the **FCS_SSHS_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE implements SSH protocol that complies with RFC(s) 4251, 4252, 4253, 4254, 4256, 4344, 6668, 8268, 8308 (Section 3.1) and 8332. The TOE implements public key authentication (SSH-RSA) and password-based authentication. The following public key algorithms are supported: ssh-rsa. The evaluator found that the public key algorithms specified in the definition of the SFR are consistent with the description within the TSS of the ST. The evaluator also found that no optional SSH characteristics are supported by the TOE. 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 **FCS_SSHS_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 SSH client's public key is compared to an authorized keys file which is stored on the TOE when establishing a user identity. 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 the sections titled **3.4.1.1.1 User Public Key Generation** and **3.10.2.1.8 User Management Commands** in the AGD titled **System Management Guide** 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 states that: **3.4.1.1.1 User Public Key Generation** Before SSH can be used with PKI, a public/private key pair must be generated. This is typically supported by the SSH client software. For example, PuTTY supports a utility called PuTTYGen that will generate key pairs. The 7705 SAR currently supports Rivest, Shamir, and Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) user public keys. The RSA public key is supported up to 4096 bits and the ECDSA public key is supported up to NIST P-521. If the client is using PuTTY, they first generate a key pair using PuTTYGen. The user sets the key type to SSH-2 RSA and sets the number of bits to be used for the key. The user can also configure a passphrase that is used to store the key locally in encrypted form. If the passphrase is configured, it acts as a password for the private key and the user must enter the passphrase in order to use the private key. If a passphrase is not used, the key is stored in plain text locally. Next, the public key must be configured for the user on the 7705 SAR with the command config>system>security>user>public-keys. The user can program the public key using the CLI or SNMP. **3.10.2.1.8 User Management Commands** public-keys Syntax public-keys Context config>system>security>user Description This command enables the context to configure public keys for SSH. rsa

Syntax rsa

Context config>system>security>user>public-keys

Description This command enables the context to configure RSA public keys.

rsa-key

Syntax rsa-key key-id [create]

no rsa-key key-id

Context config>system>security>user>public-keys>rsa

Description This command creates an RSA public key and associates it with the specified user. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.

Parameters key-id — the key identifier

Values 1 to 32

create — keyword required when first creating the RSA key. When the key is created, you can navigate into the context without the create keyword.

The same information about the using SSH public keys for SSH can be found in the section **‘Authentication’** sub-section **‘Configuring SSH Public Keys’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow:

The TOE restricts the ability to manage SSH (session keys) to security administrators via command line. The Security Administrator can modify, generate, and delete the key for SSH.
Use the commands in this section to create a new public key for SSH user authentication. The public key can be used instead of the password to authenticate the remote user.

1. Before SSH can be used with PKI, a public/private key pair must be generated. This is typically supported by the SSH client software. For example, PuTTY supports a utility called PuTTYGen that will generate key pairs. The 7705 SAR currently supports Rivest, Shamir, and Adleman (RSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) user public keys. The RSA public key is supported up to 4096 bits and the ECDSA public key is supported up to NIST P-521.

	Note: *Only the RSA keys are to be used in the CC evaluated configuration because the CC evaluated configuration does not recommend the use of ECDSA keys.* If the client is using PuTTY, they first generate a key pair using PuTTYGen. The user sets the key type to SSH-2 RSA and sets the number of bits to be used for the key. The user can also configure a passphrase that is used to store the key locally in encrypted form. If the passphrase is configured, it acts as a password for the private key and the user must enter the passphrase in order to use the private key. If a passphrase is not used, the key is stored in plain text locally. 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 **FCS_SSHS_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 the following data integrity MAC algorithms: hmac-sha1, hmac-sha2-256, hmac-sha2-512. The evaluator found that the data integrity algorithms specified in the definition of the SFR are consistent with the description within the TSS of the ST. 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 the sections titled **3.4.1.5 SSH MAC Lists, 3.9.11 Configuring SSH MAC Algorithm Lists** and **3.10.2.1.13 SSH Commands** in the AGD titled **System Management Guide** 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 states that: **3.4.1.5 SSH MAC Lists** The 7705 SAR supports configurable SSHv2 server MAC and client MAC lists that are used to negotiate the best compatible MAC algorithm between the SSH client and SSH server. Each list contains MAC algorithms and their corresponding index values, where a lower index value has a higher preference in the SSHv2 negotiation. The list is ordered by preference from highest to lowest. When the client and server exchange their MAC lists, the first algorithm in the client list that is also supported by the server is the algorithm that is agreed upon. In addition, strong HMAC algorithms can be configured at the top of the MAC list (that is, as the lowest index values in the list) in the order to be negotiated first between the client and server. The first algorithm in the list that is supported by both the client and the server is the one that is agreed upon. Note: Configurable MAC lists are only supported for SSHv2. The default list can be changed by manually removing a single index or as many indexes as required using the no mac index command. The default list can also be customized by first removing an index and then redefining it for each algorithm as required (the 7705 SAR does not support customizing an index without first removing it). **3.9.11 Configuring SSH MAC Algorithm Lists** Use the ssh command to configure SSH2 client and server MAC algorithm lists. Client MAC algorithm lists are used if the 7705 SAR is acting as an SSH client, and server MAC algorithm lists are used if the 7705 SAR is acting as an SSH server.

Note: If a 7705 SAR node is running in FIPS-140-2 mode:

- SSH1 is not supported
- for SSH2, the following MAC algorithms are not available: hmac-sha1-96, hmac-md5,

hmac-ripemd160, hmac-ripemd160-openssh-com, and hmac-mda5-96

CLI Syntax: config>system>security

ssh

client-mac-list

mac index name mac-name

server-mac-list

mac index name mac-name

3.10.2.1.13 SSH Commands

mac

Syntax mac index name mac-name

no mac index

Context config>system>security>ssh>client-mac-list

config>system>security>ssh>server-mac-list

Description This command configures the list of preferred MAC algorithms that are negotiated by an SSHv2 server or client.

Each algorithm in the list has a corresponding index value, where a lower index has a higher preference in the SSH negotiation. The list is ordered by preference from highest to lowest.

The no form of this command removes the specified MAC index from the list.

Default no mac

Parameters index — the index of the MAC algorithm in the list

	Values 1 to 255 mac-name — the algorithm for calculating the message authentication code Values Table 11 lists the default client and server MAC algorithms used for SSHv2. Note: If a 7705 SAR node is running in FIPS-140-2 mode: • SSHv1 is not supported • for SSHv2, the following MAC algorithms are not available: hmac-sha1-96, hmac-md5, hmac-ripemd160, hmac-ripemd160-openssh-com, and hmac-mda5-96. The same information about the using SSH public keys for SSH can be found in the section **'Cryptographic Protocols'** sub-section **'SSH'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow: **Note:** *If a 7705 SAR node is running in FIPS-140-2 mode:* *• SSHv1 is not supported* *• for SSHv2, the following MAC algorithms are not available: hmac-sha1-96, hmac-md5, hmac-ripemd160, hmac-ripemd160-openssh-com, and hmac-mda5-96* 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 **FCS_SSHS_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 diffie-hellman-group-14-sha1, diffie-hellman-group-14-sha256 and diffie-hellman-group-16-sha512.

	The evaluator found that the data integrity algorithms specified in the definition of the SFR are consistent with the description within the TSS of the ST. 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 the section titled **3.10.2.1.13 SSH Commands** in the AGD titled **System Management Guide** 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 states that: kex Syntax kex index name kex-name no kex index Context config>system>security>ssh>client-kex-list config>system>security>ssh>server-kex-list Description This command configures the list of preferred KEX algorithms that are negotiated by the client and server using an SSHv2 phase one handshake. By default, a KEX client and KEX server each have a hard-coded list that contains the default indexes and their corresponding algorithms. The default list can be changed by manually removing a single index or as many indexes as required using the no kex index command. The default list can also be customized by first removing an index and then redefining it for each algorithm as required. To go back to using the original hard-coded list, the default KEX indexes must be manually re-entered with their corresponding algorithms. In a KEX list, the algorithm with the lowest index value has the highest preference in the SSH

	negotiation. The list is ordered by preference from highest to lowest. When the client and server exchange their KEX lists, the first algorithm in the client list that is also supported by the server is the algorithm that is agreed upon. Note: If a 7705 SAR node is running in FIPS-140-2 mode: • SSHv1 is not supported • for SSHv2, the following KEX algorithm is not available: diffie-hellman-group1-sha The no form of this command removes the specified KEX index. Removing all the indexes from a client or server list results in an empty list, and any KEX algorithm the client or server brings to the SSHv2 negotiation will be rejected. Default no kex Parameters index — the index of the KEX algorithm in the list. The list is ordered from highest to lowest. Values 1 to 255 kex-name — the KEX algorithm for computing the shared secret key Values diffie-hellman-group16-sha512, diffie-hellman-group14-sha256, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, diffie-hellman-group1-sha1 The same information about the using SSH public keys for SSH can be found in the section **‘Cryptographic Protocols’** sub-section **‘SSH’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** 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 **FCS_SSHS_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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. The TOE verifies the following thresholds: • No longer than one hour • No more than one gigabyte of transmitted data The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey. 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 the section titled **3.10.2.1.13 SSH Commands** in the AGD titled **System Management Guide** to verify that it describes how to configure any thresholds that are configurable. Upon investigation, the evaluator found that the AGD states that: key-re-exchange Syntax key-re-exchange Context config>system>security>ssh Description This command enables the context to configure key re-exchange parameters for an SSH client or server. mbytes Syntax mbytes {mbytes | disable} no mbytes

	Context config>system>security>ssh>key-re-exchange>client config>system>security>ssh>key-re-exchange>server Description This command configures the maximum number of megabytes that can be transmitted during an SSH session before an SSH client or server initiates the key re-exchange procedure. If both the mbytes and minutes key re-exchange parameters are configured, the key re-exchange will occur at whatever limit is reached first. The no form of this command returns the setting to the default value. Default 1024 Parameters mbytes — specifies the number of megabytes that can be transmitted during an SSH session before the key re-exchange occurs Values 1 to 64000 disable — specifies that a session will never time out minutes Syntax minutes {minutes | disable} no minutes Context config>system>security>ssh>key-re-exchange>client config>system>security>ssh>key-re-exchange>server Description This command configures the maximum time that an SSH session can be up before an SSH client or server initiates the key re-exchange procedure. If both the mbytes and minutes key re-exchange parameters are configured, the key re-exchange will occur at whatever limit is reached first. The no form of this command returns the setting to the default value. Default 60 Parameters minutes — specifies the number of minutes before an SSH client or server initiates the

	key re-exchange Values 1 to 1440 disable — specifies that a session will never time out The same information about the using SSH public keys for SSH can be found in the section **'Cryptographic Protocols'** sub-section **'SSH'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5 TSS and Guidance Activities (Identification and Authentication)

5.5.1 FIA_AFL.1

5.5.1.1 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 **FIA_AFL.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 the TSS states that: When user authentication fails consecutively, the TOE locks the claimed account until the configured time has elapsed Administrators can configure the maximum number of consecutive failed authentication attempts to be between 1 and 64. Administrators may also configure the time period until the counter is reset in case of no further authentication attempts are made. The time may be configured between 0 to 60 minutes. When the account is locked, the TOE does not permit any further actions until the account is accessible. The lockout time may be configured between 0 to 1440 minutes. The authentication failures cannot lead to a situation where no administrator access is available. A user would be configured to still be granted local access to the TOE even if the remote access is denied.

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

5.5.1.2 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 **FIA_AFL.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that: The authentication failures cannot lead to a situation where no administrator access is available. A user would be configured to still be granted local access to the TOE even if the remote access is denied. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.3 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 the section titled **3.10.2.1.6 Password Commands** in the AGD titled **System Management Guide** 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 states that: attempts Syntax attempts count [time minutes1] [lockout minutes2] no attempts Context config>system>security>password

	Description This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame. If the threshold is exceeded, the user is locked out for a specified time period. If multiple attempts commands are entered, each command overwrites the previously entered command. The no attempts command resets all values to the default. Default count: 3 minutes1: 5 minutes2: 10 Parameters count — the number of unsuccessful login attempts allowed for the specified time. This is a mandatory value that must be explicitly entered. Values 1 to 64 minutes1 — the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out Values 0 to 60 minutes2 — the lockout period, in minutes, where the user is not allowed to log in Values 0 to 1440 When the user exceeds the attempted count times in the specified time, then that user is locked out from any further login attempts for the configured time period. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.1.4 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 the section titled **3.10.2.3 Clear Commands** in the AGD titled **System Management Guide** 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: lockout Syntax lockout all lockout user user-name Context admin>clear Description This command clears a security lockout for a specific user, or for all users, after they have been locked out for failing too many login attempts. Parameters all — clears lockouts for all users name — specifies a user name Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2 FIA_PMG_EXT.1

5.5.2.1 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 **FIA_PMG_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that: The TOE provides the following password management capabilities for administrator passwords:

	a) Passwords can be composed of any combination of upper and lower case letters, numbers, and the following special characters: “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”. b) Minimum password length configurable to between 6 to 50 characters. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.2.2 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 the section titled **3.10.2.2.1 Security Show Commands** in the AGD titled **System Management Guide** 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 states that: password-options Syntax password-options Context show>system>security Description This command displays configured password options. password Syntax password [password] Context config>system>security>user Description This command configures the user password for console and FTP access. Passwords must be enclosed in double quotes (" ") at the time of password creation if they contain any special characters (#, $, spaces, etc.). The double quote character (") is not accepted inside a password. It is interpreted as the start or stop delimiter of a string.

	The question mark character (?) cannot be directly inserted as input during a Telnet connection because the character is bound to the help command during a normal Telnet/console connection. To insert # or ? characters, they must be entered inside a notepad or clipboard program and then cut and pasted into the Telnet session in the password field that is encased in double quotes as delimiters for the password. If a password is entered without any parameters, a password length of zero is implied (return key). The password is stored in an encrypted format in the configuration file when specified. Parameters password — the password that must be entered by this user during the login procedure. The minimum length of the password is determined by the minimum-length command. The maximum length is as follows: • 56 characters if in unhashed plain text The unhashed plain text form must meet all the requirements that are defined within the complexity-rules command context. • 60 characters if hashed with bcrypt • from 87 to 92 characters if hashed with PBKDF2 SHA-2 • from 131 to 136 characters if hashed with PBKDF2 SHA-3 complexity-rules Syntax complexity-rules Context config>system>security>password Description This command enables the context to configure security password complexity rules. minimum-length

	Syntax minimum-length value no minimum-length Context config>system>security>password>complexity-rules Description This command configures the minimum number of characters required for passwords. If multiple minimum-length commands are entered, each command overwrites the previously entered command. The no form of the command reverts to the default value. Default 6 Parameters value — the minimum number of characters required for a password Values 6 to 50 The information about the characters that can be used for user passwords can be found in the section **‘Authentication’** sub-section **‘Password Management’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** It states that: Passwords can be composed of any combination of upper and lower case letters, numbers, and special characters that include: **[“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, [".", "_", "+"]** Minimum password lengths shall be configurable to 6 to 50 characters. The minimum password length is 6 characters. The TOE only supports the creation of strong passwords. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3 FIA_UIA_EXT.1

5.5.3.1 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 **FIA_UIA_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 TOE mandates that every user must be authenticated by accessing the local console or by remotely using SSH. Security Administrators can access the console by connecting to the console port using RJ45-DB9 or by remotely connecting to each appliance via SSHv2 Users are required to enter a username and password when remotely and locally logging into the TOE. The TOE implements RSA public key authentication via SSHv2, and password-based authentication for remote and local authentication. The user can access the TOE with correct public key-based authentication. For the password-based authentication, users must provide the correct credentials before accessing the TOE. If the user enters incorrect user credentials, they will not be allowed to access and will be presented the login page again. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3.2 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 **FIA_UIA_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 only allows limited actions prior to the user being successfully authenticated as an Administrator. The actions allowed on behalf of an unauthenticated used include viewing of the access banner at the login prompt by both local and remote users. Local users are additionally allowed to perform static route configuration, IP address configuration, FIPS Mode configuration, Auto discover/negotiation for interfaces, DNS, Duplex vs. Multiplex, and Image path configuration

	For the password-based authentication, users must provide the correct credentials before accessing the TOE. If the user enters incorrect user credentials, they will not be allowed to access and will be presented the login page again. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.3.3 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 the section titled **3.10.2.1.15 Login Control Commands** in the AGD 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 states that: pre-login-message Syntax pre-login-message login-text-string [name] no pre-login-message Context config>system>login-control Description This command creates a message displayed prior to console login attempts on the console via Telnet. Only one message can be configured. If multiple pre-login messages are configured, the last message entered overwrites the previous entry. The system name can be added to an existing message without affecting the current pre-login message. The no form of the command removes the message. Default no pre-login-message Parameters login-text-string — a text string, up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, $, spaces, etc.),

	the entire string must be enclosed within double quotes. The information about the available login methods can be found in the section **‘Authentication’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** It provides instructions on 3 available remote login methods: • Authentication using RADIUS server • Authentication using TACACS server And • Authentication using SSH. The CC guide provides details on how to configure each protocol for authentication. No configuration is required to limit the available services prior login. The evaluator did not find any services that are available for the users prior to login while conducting testing. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.4 FIA_UAU.7

5.5.4.1 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 each AGD and verified that no preparatory steps are required to ensure that authentication data is not revealed while entering the credentials. It was found during testing that the TOE does not provide any feedback while entering the password at both the directly connected and remote login prompt. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.5 FIA_X509_EXT.1/Rev

5.5.5.1 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 **FIA_X509_EXT.1/Rev** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE supports the X.509v3 certificates as defined by RFC 5280 to support authentication of external IPSEC peers. When an X.509 certificate is presented, the TOE verifies the certificate path, and certification validation process by verifying the following rules: • RFC 5280 certificate validation and certification path validation supporting a minimum path length of three certificates. • The certification path must terminate with a trusted CA certificate designated as a trust anchor. • The TOE validates a certification path by ensuring that all CA certificates in the certification path contain the basicConstraints extension with the CA flag set to TRUE. • The TOE validates the revocation status of the certificate using a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3. • The TOE validates the extendedKeyUsage field according to the following rules: ○ Server certificates presented for TLS must have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field. ○ Client certificates presented for TLS must have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field. ○ Certificates used for trusted updates and executable code integrity verification shall have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field. The TOE will only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE. When the TOE receives a remote certificate during the secure channel establishment, the validity of the remote entity certificate is verified.

	The TOE also verifies the chain of trust by validating each certificate contained in the chain and verifying that a certificate path consists of trusted CA certificates and verify the validity of the certificates. These checks are done prior to loading the certificates onto the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.5.2 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 **FIA_X509_EXT.1/Rev** entry in the section titled **TOE Summary Specification** in the Security Target 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: The use of CRL is configurable and can be used for certificate revocation. Revocation check is performed on end-entity and intermediate certificates. If the TOE is unable to establish a connection to determine the validity of a certificate, the TOE will not accept the certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.5.3 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 the sections titled **8.1.2.6 Certificate Revocation Check, 8.10.2.2.2 PKI Infrastructure Commands** and **8.10.2.2.5 Automatic CRL Update Commands** in the AGD titled **Services Guide** to verify that it contains 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 states that: **8.1.2.6 Certificate Revocation Check**

	A revocation check is a process that checks whether a certificate has been revoked by the issuer CA. The 7705 SAR supports two methods for the certificate revocation check: • CRL • OCSP The CRL can be used for both EE and CA certificate checks, while OCSP can only be used for an EE certificate check. For an IPSec application, users can configure multiple check methods with a priority order for an EE certificate. Using the status-verify command in the ipsec-tunnel configuration context, users can configure a primary method, a secondary method, and a default result. The primary and secondary methods can be either OCSP or CRL. The default result is either good or revoked. If the system does not get an answer from the primary method, it falls back to the secondary method. If the secondary method does not return an answer, the system uses the default result. By default, the system uses the CRL to check the revocation status of a certificate, whether it is an end entity certificate or a CA certificate. This makes the CRL a mandatory configuration in the ca-profile. crl-file Syntax crl-file filename no crl-file Context config>system>security>pki>ca-profile Description This command specifies the name of a file in the cf3:\system-pki\crl directory as the Certification Revoke List file of the ca-profile. The system performs the following checks against a configured crl-file when a no shutdown command is issued.

	• A valid cert-file of the ca-profile is already configured. • A configured crl-file is a DER-formatted CRLv2 file. • All mandatory fields defined in section 5.1 of RFC 5280 exist and conform to the RFC 5280-defined format. • The version field has a value of 0x1. • The delta CRL Indicator does not exist (delta CRL is not supported). • The CRL's signature is verified by using the cert-file of the ca-profile. If any of above checks fail, the no shutdown command will fail. Changing or removing the crl-file is only allowed when the ca-profile is in a shutdown state. The no form of the command removes the filename from the configuration. Default n/a Parameters filename — the name of CRL file stored in cf3:\system-pki\crl crl-update Syntax crl-update ca ca-profile-name Context admin>certificate Description This command manually initiates a CRL update for the specified CA profile. Automatic CRL update must be shutdown before this command can be issued. Default n/a Parameters ca-profile-name — the name of the CA profile file-transmission-profile Syntax file-transmission-profile name [create] no file-transmission-profile name

Context config>system

Description This command creates a new file transmission profile. The profile can be configured with transport parameters for protocols such as HTTP and additional file transmission options.

Default n/a

Parameters name — the file transmission profile name, up to 32 characters

create — keyword required when first creating the configuration context. When the

context is created, you can navigate into the context without the create keyword.

auto-crl-update

Syntax auto-crl-update [create]

no auto-crl-update

Context config>system>security>pki>ca-profile

Description This command creates the context to configure automatic CRL update parameters.

When automatic CRL update is configured and enabled with the no shutdown command,

the system downloads a CRL file from a list of configured HTTP URLs, either periodically or

before an existing CRL expires. If the downloaded CRL is a valid CRL signed by the CA and

is more recent than the existing CRL, the existing CRL is replaced.

The no form of this command deletes the automatic CRL update context and any

configurations inside it.

Default n/a

Parameters create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the create keyword.

crl-urls

Syntax crl-urls

Context config>system>security>pki>ca-prof>auto-crl-update

Description This command enables the context to configure CRL URL parameters. Up to eight URL entries can be configured under each CA profile. The configured URLs must point to a DER-encoded CRL file.

When a CRL update is initiated, the system accesses each URL in order, and the first successfully downloaded and qualified CRL is used to update the existing CRL. If the download fails or the downloaded CRL is not qualified, the system moves to the next URL in the list. If no CRL file is successfully downloaded or qualified, the system attempts to contact each URL again at the next scheduled update time (when the schedule type is configured as periodic) or after the time configured with the retry-interval command (when the schedule type is configured as next-update-based). The CRL download can be manually interrupted by issuing the shutdown command in the auto-crl-update context.

Default n/a

url-entry

Syntax url-entry entry-id [create]

no url-entry entry-id

Context config>system>security>pki>ca-prof>auto-crl-update>crl-urls

Description This command creates a new CRL URL entry or enters an existing URL entry configuration context.

The no form of this command removes the specified entry.

Default n/a

Parameters entry-id — the URL entry identifier

Values 1 to 8

create — keyword required when first creating the URL entry. When the URL entry is

created, you can navigate into the context without the create keyword.

file-transmission-profile

Syntax file-transmission-profile profile-name

no file-transmission-profile

	Context config>system>security>pki>ca-prof>auto-crl-update>crl-urls>url-entry Description This command specifies an existing file transmission profile to use when the system downloads a CRL from the configured URL in this URL entry. The profile must already be configured with the config>system>file-transmission-profile command. Automatic CRL update supports base, management, or VPRN routing instances. If VPRN is used, the HTTP server port can only be 80 or 8080. The no form of this command removes the file transmission profile name from the URL entry. The same information about CRL server configuration can be found in the section **‘X509 Certificates’**, sub-section **‘Certificate Revocation Check’** of the AGD titled **‘NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow: ***Note:*** *The 7705 SAR supports CRLs and OCSP for certificate revocation checking. However, in the FIPS-140-2 mode, in the CC evaluated configuration, only CRL server to be used for certificate revocation checks.* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.6 FIA_X509_EXT.2

5.5.6.1 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 **FIA_X509_EXT.2** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how the TOE chooses which certificates to use. Upon investigation, the evaluator found that the TSS states that: CA profiles must be created and enabled for each imported CA certificates (Root CAs and the intermediate CAs) and CRL. The Security Administrator must configure at least one trust anchor to limit the list of CA certificates. Furthermore, the Security Administrator can create a client profile to specify the cipher-list and client certificate to use. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.6.2 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 **FIA_X509_EXT.2** entry in the section titled **TOE Summary Specification** in the Security Target 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: To validate a peer certificate when CRLs are used, the Security Administrator imports its CA certificates and CRLs. CRL is used to determine whether the certificate is revoked or not. If the CRL cannot be obtained, then the TOE will reject the certificate. Revocation check is performed on end-entity and intermediate certificates. If the TOE is unable to establish a connection to determine the validity of a certificate, the TOE will not accept the certificate. Next, the evaluator examined the section titled **8.10.2.2.2 PKI Infrastructure Commands** in the AGD titled **Services Guide** to verify that it describes the expected behavior of the TOE when the validity of peer certificates cannot be determined. Upon investigation, the evaluator found that the AGD states that: crl-file Syntax crl-file filename no crl-file Context config>system>security>pki>ca-profile Description This command specifies the name of a file in the cf3:\system-pki\crl directory as the Certification Revoke List file of the ca-profile. The system performs the following checks against a configured crl-file when a no shutdown command is issued. • A valid cert-file of the ca-profile is already configured. • A configured crl-file is a DER-formatted CRLv2 file. • All mandatory fields defined in section 5.1 of RFC 5280 exist and conform to the RFC 5280-defined format.

• The version field has a value of 0x1.

• The delta CRL Indicator does not exist (delta CRL is not supported).

• The CRL's signature is verified by using the cert-file of the ca-profile.

If any of above checks fail, the no shutdown command will fail.

Changing or removing the crl-file is only allowed when the ca-profile is in a shutdown state.

The no form of the command removes the filename from the configuration.

Default n/a

Parameters filename — the name of CRL file stored in cf3:\system-pki\crl

The same information about the expected behavior of the TOE when the validity of peer certificates cannot be determined is included in the section **'X509 Certificates',** sub-section **'CRL Configuration'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow:

<u>Automatic CRL Update Commands</u>

- **crl-update**
  Syntax: crl-update ca *ca-profile-name*
  Context: admin>certificate
  Description: This command manually initiates a CRL update for the specified CA profile.
  Automatic CRL update must be shutdown before this command can be issued.
  Default: n/a
  Parameters: *ca-profile-name* — the name of the CA profile

- **auto-crl-update**
  Syntax: auto-crl-update [create]
  no auto-crl-update
  Context: config>system>security>pki>ca-profile

	Description: This command creates the context to configure automatic CRL update parameters. When automatic CRL update is configured and enabled with the no shutdown command, the system downloads a CRL file from a list of configured HTTP URLs, either periodically or before an existing CRL expires. If the downloaded CRL is a valid CRL signed by the CA and is more recent than the existing CRL, the existing CRL is replaced.The no form of this command deletes the automatic CRL update context and any configurations inside it. **Default:** n/a **Parameters:** create — keyword required when first creating the configuration context. When the context is created, you can navigate into the context without the create keyword. In the sub-section **'Certificate Revocation Check',** the following information is stated: __**Certificate Revocation Check**__ • A revocation check is a process that checks whether a certificate has been revoked by the issuer CA. The 7705 SAR supports revocation check using CRL (as specified in RFC 5280 Section 6.3). • The CRL can be used for both EE and CA certificate checks. By default, the system uses the CRL to check the revocation status of a certificate, whether it is an end entity certificate or a CA certificate. This makes the CRL a mandatory configuration in the ca-profile. • In CC mode, the audo-crl-update must be enabled (ie. Periodic queries to a remote CRL server should be made by the TOE that is in the CC evaluated configuration). • If the CRL server is unreachable, the TOE will not accept the certificates. • If the issuer is not present, or if the issuer certificate does not have the CA:true flag in the basicConstraints section, the validation fails. The TOE verifies the validity of the signature. If the signature is not valid, the validation fails. It then confirms that the current date and time is within the valid time period specified in the certificate. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.6.3 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. 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 the sections titled **8.1.2 X.509v3 Certificate Overview**, **8.10.2.2.1 X.509 and Certificate Commands** and **8.10.2.2.4 IKE PKI Commands** in the AGD titled **Services Guide** 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 states that: In addition to issuing certificates, the public key infrastructure (PKI) also includes a mechanism for revoking certificates due to reasons such as a compromised private key. A certificate can be used for authentication. Typically, the certificate authentication process functions as follows. • The system trusts a CA as the trust anchor CA (which typically is a root CA). This means that all certificates issued by a trust anchor CA, or the certificates issued by a subordinate CA that have been issued by the trust anchor CA, are consider trusted. • A peer that is to be authenticated presents its certificate along with a signature over some shared data between the peer and system, and the certificate is signed using a private key. • The signature is verified by using the public key in the certificate. In addition, the certificate itself is verified as being issued by the trust anchor CA or a subordinate CA that is part of the chain leading up to the trust anchor CA. The system can also check if the peer's certificate has been revoked. Only when all these verifications succeed does the certificate authentication succeed. The evaluator observed the subsequent steps and found that each AGD included all the steps for configuring the operating environment. The same information about the operating environment necessary for the TOE to use certificates is included in the section **'X509 Certificates',** sub-section **'CRL Configuration'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow: **Certificate Revocation Check** • A revocation check is a process that checks whether a certificate has been revoked by the issuer CA. The 7705 SAR supports revocation check using CRL (as specified in RFC 5280 Section 6.3). • The CRL can be used for both EE and CA certificate checks. By default, the system uses the CRL to check the revocation status of a certificate, whether it is an end entity certificate or a CA certificate. This makes the CRL a mandatory configuration in the ca-profile.

	• In CC mode, the audo-crl-update must be enabled (ie. Periodic queries to a remote CRL server should be made by the TOE that is in the CC evaluated configuration). • If the CRL server is unreachable, the TOE will not accept the certificates. • If the issuer is not present, or if the issuer certificate does not have the CA:true flag in the basicConstraints section, the validation fails. The TOE verifies the validity of the signature. If the signature is not valid, the validation fails. It then confirms that the current date and time is within the valid time period specified in the certificate. ***Note:*** *The 7705 SAR supports CRLs and OCSP for certificate revocation checking. However, in the FIPS-140-2 mode, in the CC evaluated configuration, only CRL server to be used for certificate revocation checks.* **1. CRL Configuration** Use a web server (Example Apache 2) to host the CRL files on the CRL server which the TOE can then retrieve via HTTP. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.6.4 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 the section titled **8.2.7 Automatic CRL Update** in the AGD titled **Services Guide** 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 AGD states that Up to eight URL entries can be configured under each CA profile. The configured URLs must point to a DER-encoded CRL file. When a CRL update is initiated, the system accesses each URL in order, and the first successfully downloaded and qualified CRL is used to update the existing CRL. If the download fails or the downloaded CRL is not qualified, the system moves to the next URL in the list. If no CRL can be downloaded or qualified, the system attempts to contact each URL again at the next scheduled update time (when the schedule type is periodic) or after the time configured with the retry-interval command (when the schedule type is next-update-based).

	A CRL update is initiated immediately if auto-crl-update is enabled and the system detects that the configured CRL file does not exist, or is invalid or expired, or if the schedule type is configured as next-update-based and the scheduled update time has already passed. A CRL update can be initiated manually with the admin>certificate>crl-update command, but automatic CRL update must first be shut down. The same information about the operating environment necessary for the TOE to use certificates is included in the section **'X509 Certificates',** sub-section **'CRL Configuration'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow: **Certificate Revocation Check** • A revocation check is a process that checks whether a certificate has been revoked by the issuer CA. The 7705 SAR supports revocation check using CRL (as specified in RFC 5280 Section 6.3). • The CRL can be used for both EE and CA certificate checks. By default, the system uses the CRL to check the revocation status of a certificate, whether it is an end entity certificate or a CA certificate. This makes the CRL a mandatory configuration in the ca-profile. • In CC mode, the audo-crl-update must be enabled (ie. Periodic queries to a remote CRL server should be made by the TOE that is in the CC evaluated configuration). • If the CRL server is unreachable, the TOE will not accept the certificates. • If the issuer is not present, or if the issuer certificate does not have the CA:true flag in the basicConstraints section, the validation fails. The TOE verifies the validity of the signature. If the signature is not valid, the validation fails. It then confirms that the current date and time is within the valid time period specified in the certificate. The default action is non-configurable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.7 FIA_X509_EXT.3

5.5.7.1 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 **FIA_X509_EXT.3** SFR in the ST and verified that “device-specific information” is not selected. Therefore, this assurance activity is not applicable. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.5.7.2 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 the section titled **8.10.2.2.1 X.509 and Certificate Commands** in the AGD titled **Services Guide** 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 states that: gen-local-cert-req Syntax gen-local-cert-req keypair url-string subject-dn subject-dn [domain-name domain-name] [ip-addr {ip-address}] file url-string [hash-alg hash-algorithm] [useprintable] Context admin>certificate Description This command generates a PKCS# 10 formatted certificate request by using a local existing key pair file. Default n/a Parameters url-string — the name of the key file in cf3:\system-pki\key that is used to generate a certificate request Values url-string : local-url, 99 characters maximum

	local-url : cflash-id/file-path cflash-id : cf1:, cf2:, cf3: subject-dn — the distinguishing name that is used as the subject in a certificate request, including: • C – Country • ST – State • O – Organization name • OU – Organization Unit name • CN – common name This parameter is formatted as a text string including any of the above attributes. The attribute and its value are linked by using "=", and "," is used to separate different attributes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6 TSS and Guidance Activities (Security Management)

5.6.1 FMT_MOF.1/ManualUpdate

5.6.1.1 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 the section titled **5.1.1 Configuration and Image Loading**, **5.3.1 Before Upgrading**, **5.3.2 Performing the Upgrade, 5.12 Service Management Tasks** and **5.13.2.1 Configuration Commands** in the AGD titled **Basic System Configuration Guide** to verify that it describes any necessary steps to perform manual update. Upon investigation, the evaluator found that the AGD states that:

	Nokia recommends that the boot loader file on all 7705 SAR platforms be upgraded using a specific command. This command is mandatory on all 7705 SAR platforms that do not have a removable compact flash drive and is part of a mechanism that protects the boot loader file from accidental overwrites on these platforms. The command checks that the new boot.ldr file is a valid image and that it is at least a minimum supported variant for the hardware platform on which it is being loaded. Once this has been verified, the command overwrites the boot.ldr file that is stored on the system. The evaluator found that the above mentioned sections describe the process of manually updating the software on the TOE. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2 FMT_FMT_MOF.1/Functions

5.6.2.1 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 **FMT_MOF.1/Functions** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS identifies 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). Upon investigation, the evaluator found that the TSS states that: The TOE restricts the ability to modify the behavior of transmission of audit data to an audit server to Security Administrators. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.2.2 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 device does not support this functionality

	Based on these findings, this assurance activity is considered not applicable.
Verdict	NA

5.6.3 FMT_MOF.1/Services

5.6.3.1 FMT_MOF.1/Services TSS 2

Objective	For non-distributed TOEs, the evaluator shall ensure the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	The evaluator examined the **FMT_MOF.1/Services** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the TSS states that: The Security Administrator may use the CLI to start and stop the services. The following services may be started and stopped: • SSH server • SFTP server • SNMP • Logging to file, memory, syslog • IPSec tunnels • RADIUS • TACACS+ Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.3.2 FMT_MOF.1/Services Guidance 2

Objective	For non-distributed TOEs, the evaluator shall also ensure the Guidance Documentation describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed.
Evaluator Findings	The evaluator examined the section titled **5.4 Accessing the CLI** and the sub-sections titled **5.4.2 Telnet Connection 5.4.3 SSH Connection, 6.10.6.1 Disconnect** and **6.13.2.2.1 System Administration Commands** in the AGD titled **Basic System Configuration Guide**, sections titled **3.10.2.1.15 Login Control Commands, 3.10.2.1.8 User Management Commands, 5.2 Log Destinations, 5.7 Log Configuration Overview, 5.10 Common Configuration Tasks, 5.10.1 Configuring an Event Log, 3.10.2.1.13 SSH Commands, 3.10.2.1.10 RADIUS Client Commands, 3.9.13 RADIUS Configurations, 3.10.2.1.11 TACACS+ Client Commands**, **3.9.14 TACACS+ Configurations** in the AGD titled **System Management Guide** and sections titled **8.5 Configuring IPSec with CLI**, **8.9.5 Deleting an IPSec Tunnel, 8.2**

Public Key Infrastructure (PKI), 8.2.1 CA Role in PKI, 8.2.7 Automatic CRL Update and **8.10.1.2 PKI Configuration Commands** to verify that it describes how the TSS lists the services the Security Administrator is able to start and stop and how that how that operation is performed. Upon investigation, the evaluator found that the AGD states that:

5.4 Accessing the CLI

There are three ways to access management of the 7705 SAR:

- console connection
- Telnet connection
- SSH connection

To access the CLI to configure the software for the first time, follow these steps:

1. Ensure that the CSM is installed and power to the chassis is turned on. The 7705 SAR software then automatically begins the boot sequence.
2. When the boot loader and BOF image and configuration files are successfully located, establish a router connection (console session).

6.10.6.1 Disconnect

The disconnect command immediately disconnects a user from a console, Telnet, FTP, SSH, SFTP, or MPT craft terminal (MCT) session. The ssh keyword disconnects users connected to the node via SSH or SFTP.

Note: Configuration modifications are saved to the primary image file.

CLI Syntax: admin

disconnect [address ip-address | username user-name |

{console | telnet | ftp | ssh | mct}]

Example: admin# disconnect

The following example displays the disconnect command results.

ALU-1>admin# disconnect

ALU-1>admin# Logged out by the administrator

Connection to host lost.

3.10.2.1.8 User Management Commands

access

Syntax [no] access [ftp] [snmp] [console]

[no] access [ftp] [console]

Context config>system>security>user

config>system>security>user-template

Description This command grants a user permission for FTP, SNMP, or console access.

If a user requires access to more than one application, then multiple applications can be specified in a single command. Multiple commands are treated sequentially.

The no form of the command removes access for a specific application.

The no access command denies permission for all management access methods. To deny a single access method, enter the no form of the command followed by the method to be denied; for example, no access ftp denies FTP access.

Default no access

Parameters ftp — specifies FTP permission

snmp — specifies SNMP permission. This keyword is only configurable in the config>system>security>user context.

console — specifies console access (serial port or Telnet) permission

snmp

Syntax snmp

Context config>system>security>user

Description This command enables the context to configure SNMP group membership for a specific user and defines encryption and authentication parameters.

All SNMPv3 users must be configured with the commands available in this CLI context.

The 7705 SAR always uses the configured SNMPv3 user name as the security user name.

5.2 Log Destinations

Both event logs and accounting logs use a common mechanism for referencing a log destination. The 7705 SAR supports the following log destinations:

- Console
- Session
- Memory Logs
- Log Files
- SNMP Trap Group
- Syslog

5.10.1 Configuring an Event Log

```
CLI Syntax: config>log
log-id log-id
description description-string
filter filter-id
from {[main] [security] [change] [debug-trace]}
to console
to file log-file-id
to memory [size]
to session
to snmp [size]
to syslog syslog-id
time-format {local | utc}
```

no shutdown

3.10.2.1.10 RADIUS Client Commands

radius

Syntax [no] radius

Context config>system>security

Description This command enables the context to configure RADIUS authentication on the 7705 SAR.

For redundancy, multiple server addresses can be configured for each 7705 SAR.

The no form of the command removes the RADIUS configuration.

3.10.2.1.11 TACACS+ Client Commands

tacplus

Syntax [no] tacplus

Context config>system>security

Description This command enables the context to configure TACACS+ authentication on the 7705 SAR.

For redundancy, multiple server addresses can be configured for each 7705 SAR.

The no form of the command removes the TACACS+ configuration.

8.7.4 Configuring IPSec and IPSec Tunnels in Services

IPSec is configured under IES and VPRN services. For the private-side IPSec tunnel interface and SAP, under the VPRN service context, configure IPSec security policies, and create tunnel interfaces, private tunnel SAPs, IPSec tunnels, and IPSec tunnel parameters. The tunnel keyword must be used when creating an interface for a private tunnel SAP. For a public-side IPSec tunnel interface and SAP, under the IES or VPRN service context, create an interface and public tunnel SAP. The tunnel keyword is not used when creating an interface for a public tunnel SAP. Private-side and public-side tunnels function in pairs, where a pair is defined by the service ID and the interface subnet. The local gateway address and delivery service configured using the VPRN ipsec-tunnel>local-gateway-address command correspond to the IES or VPRN interface address and service ID where the public-side tunnel interface is defined.

8.9.5 Deleting an IPSec Tunnel

	IPSec tunnels are created under the VPRN service. Although an IPSec tunnel is created on the private side of the tunnel in the CLI, the configuration itself is general and can apply to either the public or private side of the tunnel. To delete an IPSec tunnel: CLI Syntax: config>service>vprn>if>sap# no ipsec-tunnel ipsectunnel-name Example: config>service>vprn>if>sap# no ipsec-tunnel ies_tunnelPublicSide_1 Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4 FMT_MTD.1/CoreData

5.6.4.1 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 **FMT_MTD.1/CoreData** entry in the section titled **TOE Summary Specification** in the Security Target 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: Accesses available to unauthenticated users depend on the access methods. When accessing the TOE remotely, the unauthenticated user is only allowed to view the TOE access banner and login prompts. For the users accessing the TOE locally, the TOE allows viewing of the access banner and the login prompts but also allows the user to access basic configuration tasks of the TOE, including Static route configuration, IP address configuration, FIPS Mode configuration, Auto discover/negotiation for interfaces, DNS, Duplex vs. Multiplex, and Image path configuration.

	The evaluator examined the **FMT_MTD.1/CoreData** entry in the section titled **TOE Summary Specification** in the Security Target 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 (RBAC). Only the role Security Administrator is implemented. When a user with sufficient credentials is successfully authenticated, the user shall enter the role Security Administrator. Only Security Administrators can manage the certificates in TOE's trust store. Security Administrator role is associated with a set of defined access rights that are granted to a user entering the role. The access rights grant the user a right to access TOE data and functions. The TOE prevents users not assigned to the Security Administrator role from accessing the TOE data and functions requiring Security Administrator access rights. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4.2 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 **FMT_MTD.1/CoreData** entry in the section titled **TOE Summary Specification** in the Security Target 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 implements active and inactive trust stores. Trust stores in the volatile memory are active. Inactive trust stores reside in the persistent store in the form of files. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4.3 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 the following sections in each 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 each AGD includes configuration of the following in the respective sections:

	• **Audit Configuration** ○ *Sections titled ‘5.6 Configuring Logging with CLI’ and ‘5.12 Log Command Reference’* • **Identification/Authentication** ○ *Sections titled ‘3.10.2.1.8 User Management Commands’, ‘3.10.2.1.6 Password Commands’, ‘10.2.1.8 User Management Commands’, ‘3.10.2.1.10 RADIUS Client Commands’, ‘3.10.2.1.11 TACACS+ Client Commands’* • **SSH configuration** ○ *Section titled ‘3.10.2.1.13 SSH Commands’* • **IPsec configuration** ○ *Section titled ‘8.10.2.1 IPSec Configuration Commands’,’ 8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands’* • **Time stamps** ○ *Section titled ‘6.10.6.2 Set-time’, ‘6.13.2.1.5 System Time Commands’* • **Session time-out** ○ *Section titled ‘3.10.2.1.15 Login Control Commands’* • **TOE Banner** ○ *Section titled ‘3.10.2.1.15 Login Control Commands’* • **TOE updates** ○ *Sections titled ‘5.1.1 Configuration and Image Loading’,’5.3.1 Before Upgrading’,’ 5.3.2 Performing the Upgrade’,’5.12 Service Management Tasks’ and ‘5.13.2.1 Configuration Commands’* • **X.509 Certificates** ○ *Section titled ‘8.10.2.2.1 X.509 and Certificate Commands’* The evaluator found that this encompasses all the TSF-data manipulating functionality required by the NDcPP. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.4.4 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 the sections titled **8.2.3 Certificate Storage** and **8.7.6 Configuring X.509v3 Certificate Parameters** in the AGD titled **Services Guide** 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 states that:

The 7705 SAR IPSec configuration expects the keys and certificates to be stored in

a particular directory on the 7705 SAR compact flash. This directory is called

cf3:\system-pki and is created automatically when the first file is imported into this

folder.

The following files can be imported and exported to and from the cf3:\system-pki

directory. An example of the directory is shown after the list.

• key pair – this file is encrypted during the import process

• certificates

• certificate revocation list (CRL)

The evaluator examined the sections titled **8.10.2.2.1 X.509 and Certificate Commands, 8.1.4 Trust Anchor Profile** and **8.10.2.2.3 IPSec PKI Commands** in the AGD titled **Services Guide** 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 states that:

import

Syntax import type {cert | key | crl} input url-string output filename format input-format [password

password]

Context admin>certificate

Description This command converts an input file (either key, certificate, or CRL) to a system format file.

The following list summarizes the formats supported by this command.

• Certificate

- PKCS #12

- PKCS #7 PEM encoded

- PKCS #7 DER encoded

	- PEM - DER • Key - PKCS #12 - PEM - DER • CRL - PKCS #7 PEM encoded - PKCS #7 DER encoded - PEM - DER If there are multiple objects with same type in the input file, only the first object will be extracted and converted. Default n/a Parameters input url-string — the URL for the input file. This URL could be either a local compact flash URL file or an FTP URL to download the input file. output filename — the name of output file, up to 95 characters in length. The output directory depends on the file type: • Key: cf3:\system-pki\key • Cert: cf3:\system-pki\cert • CRL: cf3:\system-pki\CRL Values url-string : local-url, 99 characters maximum local-url : cflash-id/file-path cflash-id : cf1:, cf2:, cf3: type — the type of input file

	Values cert, key, crl input-format — the format of the input file Values pkcs12, pkcs7-der, pkcs7-pem, pem, der password — the password to decrypt the input file if it is an encrypted PKCS# 12 file, up to 32 characters **8.1.4 Trust Anchor Profile** The 7705 SAR supports multiple trust anchors for each IPSec tunnel. A trust anchor profile can be configured with up to eight CAs. The system builds a certificate chain by using the certificate in the first certificate payload in the received IKEv2 message. If any of the configured trust anchor CAs in the trust anchor profile appear in the chain, then authentication is successful; otherwise, authentication fails. **8.10.2.2.3 IPSec PKI Commands** trust-anchor-profile Syntax trust-anchor-profile name [create] no trust-anchor-profile name Context config>ipsec Description This command specifies the trust-anchor-profile for the IPSec tunnel. This command will override the trust-anchor-profile configuration in the config>service>vprn>if>sap>ipsec-tunnel>cert context. Default no trust-anchor-profile Parameters profile-name — the trust-anchor-profile name Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5 FMT_MTD.1/CryptoKeys

5.6.5.1 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 **FMT_MTD.1/CryptoKeys** entry in the section titled **TOE Summary Specification** in the Security Target 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: The Security Administrator has the ability to modify, generate, and delete SSH and IPsec session keys as well as any configured X.509 certificates. The key management functions are performed through the Command Line Interface and not accessible to users in other roles. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.5.2 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 the section titled **3.10.2.1.8 User Management Commands** in the AGD titled **System Management Guide and** the section titled **8.10.2.2.1 X.509 and Certificate Commands** in the AGD titled **Services Guide** 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 states that: **3.10.2.1.8 User Management Commands** rsa Syntax rsa Context config>system>security>user>public-keys Description This command enables the context to configure RSA public keys.

rsa-key

Syntax rsa-key key-id [create]

no rsa-key key-id

Context config>system>security>user>public-keys>rsa

Description This command creates an RSA public key and associates it with the specified user. Multiple public keys can be associated with the user. The key ID is used to identify these keys for the user.

Parameters key-id — the key identifier

Values 1 to 32

create — keyword required when first creating the RSA key. When the key is created, you can navigate into the context without the create keyword

8.10.2.2.1 X.509 and Certificate Commands

gen-keypair

Syntax gen-keypair url-string [size {512 | 1024 | 2048}] [type {rsa | dsa}]

Context admin>certificate

Description This command generates an RSA or DSA private key/public key pair and stores it in a local file in the cf3:\system-pki\key directory.

Parameters url-string — the name of the key file

Values url-string : local-url, 99 characters maximum

local-url : cflash-id/file-path

cflash-id : cf1:, cf2:, cf3:

size — the key size in bits (the minimum key size is 1024 bits when running in FIPS-140-

2 mode)

Values 512, 1024, or 2048

Default 2048

type — the type of key

	Values rsa, dsa Default rsa import Syntax import type {cert | key | crl} input url-string output filename format input-format [password password] Context admin>certificate Description This command converts an input file (either key, certificate, or CRL) to a system format file. The following list summarizes the formats supported by this command. • Certificate - PKCS #12 - PKCS #7 PEM encoded - PKCS #7 DER encoded - PEM - DER • Key - PKCS #12 - PEM - DER • CRL - PKCS #7 PEM encoded - PKCS #7 DER encoded - PEM - DER

	If there are multiple objects with same type in the input file, only the first object will be extracted and converted. Default n/a Parameters input url-string — the URL for the input file. This URL could be either a local compact flash URL file or an FTP URL to download the input file. output filename — the name of output file, up to 95 characters in length. The output directory depends on the file type: • Key: cf3:\system-pki\key • Cert: cf3:\system-pki\cert • CRL: cf3:\system-pki\CRL Values url-string : local-url, 99 characters maximum local-url : cflash-id/file-path cflash-id : cf1:, cf2:, cf3: type — the type of input file Values cert, key, crl input-format — the format of the input file Values pkcs12, pkcs7-der, pkcs7-pem, pem, der password — the password to decrypt the input file if it is an encrypted PKCS# 12 file, up to 32 characters The same information about configuring the x509 certificates can be found in the section **'X509 Certificates'** of the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, this CC guide also includes the following additional guidance statements for administrators to follow: **<u>Note:</u>** *The key sizes 512 and 1024 are not supported in FIPS mode. The DSA key pairs should not be configured in the CC evaluated configuration. The minimum key size is 2048 bits in FIPS mode.*

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

5.6.6 FMT_SMF.1

5.6.6.1 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 the **FMT_SMF.1** entry in the section titled **TOE Summary Specification** in the TSS to verify that it details which security management functions are available through which interface(s). Upon investigation, the evaluator mentioned the respective sections in AGD for the points stated in the TSS as below: The *TOE* only implements the role Security Administrator. The TOE can be accessed by users assigned to the role Security Administrator through a Command Line Interface locally from console or remotely over SSH. The Administrator can perform the following management functions: • **Ability to administer the TOE locally and remotely;** ○ *Section titled '5.4 Accessing the CLI' and '6.13.2.2.1 System Administration Commands'* • **Ability to configure the access banner;** ○ *Section titled '3.10.2.1.15 Login Control Commands'* • **Ability to configure the session inactivity time before session termination or locking;** ○ *Section titled '3.10.2.1.15 Login Control Commands'* • **Ability to update the TOE, and to verify the updates using hash comparison prior to installing those updates;** ○ *Sections titled '5.1.1 Configuration and Image Loading','5.3.1 Before Upgrading',' 5.3.2 Performing the Upgrade','5.12 Service Management Tasks', '5.13.2.1 Configuration Commands' and '5.1.3 FIPS-140-2 Mode'* • **Ability to configure the authentication failure parameters for FIA_AFL.1;** ○ *Sections titled '3.10.2.1.8 User Management Commands', '3.10.2.1.6 Password Commands', '10.2.1.8 User Management Commands', '3.10.2.1.10 RADIUS Client Commands', '3.10.2.1.11 TACACS+ Client Commands'* • **Ability to start and stop services;**

	○ *Sections titled '5.4 Accessing the CLI', '5.4.2 Telnet Connection', '5.4.3 SSH Connection', '6.10.6.1 Disconnect', '6.13.2.2.1 System Administration Commands', ' 3.10.2.1.15 Login Control Commands', '3.10.2.1.8 User Management Commands', '5.2 Log Destinations', '5.7 Log Configuration Overview', '5.10 Common Configuration Tasks', '5.10.1 Configuring an Event Log', '3.10.2.1.13 SSH Commands', '3.10.2.1.10 RADIUS Client Commands', '3.9.13 RADIUS Configurations', '3.10.2.1.11 TACACS+ Client Commands', '3.9.14 TACACS+ Configurations', '8.5 Configuring IPSec with CLI', '8.9.5 Deleting an IPSec Tunnel', '8.2 Public Key Infrastructure (PKI)', '8.2.1 CA Role in PKI', '8.2.7 Automatic CRL Update' and '8.10.1.2 PKI Configuration Commands'* • **Ability to configure audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full);** ○ *Sections titled '5.2 Log Destinations', '5.6 Configuring Logging with CLI', '5.12 Log Command Reference', '5.12.2.1 Configuration Commands'* • **Ability to modify the behaviour of the transmission of audit data to an external IT entity;** ○ *Sections titled '5.2.6 Syslog', '5.10.7 Configuring a Syslog Target', '5.11 Log Management Tasks', '5.11.5 Modifying a Syslog ID' and '5.11.6 Deleting a Syslog ID'* • **Ability to manage the cryptographic keys;** ○ *Sections titled '3.10.2.1.8 User Management Commands' and '8.10.2.2.1 X.509 and Certificate Commands'* • **Ability to configure the cryptographic functionality;** ○ *Sections titled '3.10.2.1.8 User Management Commands' and '8.10.2.2.1 X.509 and Certificate Commands'* • **Ability to configure thresholds for SSH rekeying;** ○ *Section titled '3.10.2.1.13 SSH Commands'* • **Ability to configure the lifetime for IPsec SAs;** ○ *Section titled '8.10.2.1 IPSec Configuration Commands',' 8.10.2.1.3 Internet Key Exchange (IKE) and Transform Commands'* • **Ability to re-enable an Administrator account;** ○ *Section titled '3.10.2.1.15 Login Control Commands'* • **Ability to set the time which is used for time-stamps;** ○ *Section titled '6.10.6.2 Set-time', '6.13.2.1.5 System Time Commands'* • **Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors; and** ○ *8.10.2.2.3 IPSec PKI Commands* • **Ability to import X.509v3 certificates to the TOE's trust store.** ○ *Section titled '8.10.2.2.1 X.509 and Certificate Commands'* **Information about TSF-initiated Termination is covered in the TSS under FTA_SSL_EXT.1 or FTA_SSL.3.**

	In addition to the above, the TSS directs the reader to the FTA_SSL_EXT.1 or FTA_SSL.3 TSS entries for information on managing TSF-initiated termination. The management guidance for these SFRs is provided in the appropriate FTA_SSL_EXT.1 and FTA_SSL.3 assurance activities. The AGD describes the local interface in the sections titled '5.4 Accessing the CLI' and '6.13.2.2.1 System Administration Commands' All of the above information is available in the CC guide titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** In addition, the section '**Cryptographic Protocols'** sub-section **'IPSec'** of this CC guide includes the following additional guidance statements for administrators to follow: • **Ability to configure the reference identifier for the peer;** **3. <u>Configuring Reference Identifiers</u>** • <u>The TOE supports the following reference identifiers</u>: ○ SAN: IP address ○ SAN: FullyQualifiedDomainName (FQDN) ○ SAN: user FQDN • <u>The following configuration is used to configure reference identifiers on the device</u>: remote-id type <ipv4, fqdn, email> value *value* Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.6.2 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 the section **‘Administration using local console and SSH’,** sub-section **‘Accessing the CLI’** in the AGD titled ‘**NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide’** to verify that it describes the local administrative interface.

There are two ways to access management of the 7705 SAR:

- Console connection
- SSH connection

To access the CLI and configure the software for the first time, follow these steps:

1. Ensure that the CSM is installed and power to the chassis is turned on. The 7705 SAR software then automatically begins the boot sequence.

2. When the boot loader and BOF image and configuration files are successfully located, establish a router connection (console session).

- Assign a name to the device using the following command:

```
*A:SR-xx# configure system name <system-name>
```

- Assign the IP address to the management interface using the following command:

```
*A:SR-xx# bof address <ip-prefix/ip-prefix-length>"active"
```

To establish a console connection:

Step 1. Connect the terminal to the Console port on the front panel using the serial cable.

Step 2. Power on the terminal.

Step 3. Establish the connection by pressing the <Enter> key a few times on your terminal keyboard.

Step 4. At the router prompt, enter the login and password.

The default login is admin.

The default password is admin.

To disconnect from a console session, use the following command:

	- **logout** **Syntax**: logout **Context**: <global> **Description**: This command logs out of the router session. When the logout command is issued from the console, the login prompt is displayed and any log IDs directed to the console are discarded. When the console session resumes (regardless of the user), the log output to the console resumes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.7 FMT_SMR.2

5.6.7.1 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 the **FMT_SMR.2** entry in section titled **TOE Summary Specification** in the TSS 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 maintains a single role, Security Administrator. Each user is identified with a username and authenticated with a password prior to being assigned to a role. Only successfully authenticated users shall be assigned to roles. User assigned to the role Security Administrator may administer the TOE locally and remotely. Local access is via console, remote access is over SSH. Admins can configure user's privilege that grant or deny privilege to users from login access via Console and Remote access. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.6.7.2 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.

<table>
<tr><td>Evaluator Findings</td><td>The evaluator examined the section titled <b>5.4.1 Console Connection, 6.13.2.2.1 System Administration Commands</b> and <b>3.11.2.1 Basic CLI Commands</b> in the AGD titled <b>Basic System Configuration Guide</b> 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:
<b>5.4.1 Console Connection</b>
To establish a console connection:
Step 1. Connect the terminal to the Console port on the front panel (Figure 10)
using the serial cable.
Step 2. Power on the terminal.
Step 3. Establish the connection by pressing the <Enter> key a few times on your
terminal keyboard.
Step 4. At the router prompt, enter the login and password.
The default login is admin.
The default password is admin.
<b>6.13.2.2.1 System Administration Commands</b>
admin
Syntax admin
Context <ROOT>
Description This command enables the context to configure administrative system commands. Only authorized users can execute the commands in the admin context.
Default n/a
<b>3.11.2.1 Basic CLI Commands</b>
ssh
Syntax ssh host [-l username] [-v ssh-version] [router router-instance | service-name service-name] [re-exchange-min minutes] [re-exchange-mbyte megabytes]
Context <global></td></tr>
</table>

	Description This command opens a Secure Shell (SSH) session with another host. This command initiates a client SSH session with the remote host and is independent from the administrative or operational state of the SSH server. However, to be the target of an SSH or SFTP session, the SSH server must be operational. The command also allows the user to initiate an SSH session with a key re-exchange to occur after a specified number of minutes have passed or a specified number of megabytes have been transmitted. If both parameters are configured, the key re-exchange will occur at whatever limit is reached first. If neither parameter is set, key re-exchange will not occur. Quitting SSH while in the process of authentication is accomplished by either executing a <Ctrl-c> or "~." (tilde and dot), assuming the “~” is the default escape character for the SSH session. Parameters host — the remote host for an SSH session. The IP address, DNS name (if DNS name resolution is configured), or the user name at the IP address can be specified. Values [user@]hostname: 255 characters maximum user: user name, 32 characters maximum hostname: [dns-name | ipv4-address | ipv6-address] dns-name: 128 characters maximum ipv4-address a.b.c.d Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7 TSS and Guidance Activities (Protection of the TSF)

5.7.1 FPT_APW_EXT.1

5.7.1.1 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 **FPT_APW_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: The passwords are stored in files in non-reversible hashes. This ensures that they cannot be recovered from the files. When a password is read from the CLI, it is hashed and the hash is compared to the reference value stored in the password file. This ensures that the passwords are not stored in plaintext. The evaluator also examined the **FPT_APW_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: When a password is read from the CLI, it is hashed and the hash is compared to the reference value stored in the password file. This ensures that the passwords are not stored in plaintext. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.2 FPT_SKP_EXT.1

5.7.2.1 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 **FPT_STM_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE stores all private keys in a secure storage and is not accessible through an interface to administrators.

	The Table 17 of the ST also contains detailed information regarding the storage location and method of each type of key. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3 FPT_STM_EXT.1

5.7.3.1 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 **FPT_STM_EXT.1** SFR in the ST and verified that it describes the use of time, and that it provides a description of how the time is maintained. The TSS states that: The TOE provides reliable time stamps. The clock function is reliant on the system clock provided by the underlying hardware. The clock is utilized for providing reliable time stamps used in the following functions: • Audit events • Session inactivity • X.509 certificate expiration validation. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.3.2 FPT_STM_EXT.1 TSS 2 **[TD0632]**

Objective	If “obtain time from the underlying virtualization system” is selected, the evaluator shall examine the TSS to ensure that it identifies the VS interface the TOE uses to obtain time. If there is a delay between updates to the time on the VS and updating the time on the TOE, the TSS shall identify the maximum possible delay.
Evaluator Findings	The evaluator examined the **FPT_STM_EXT.1** SFR in the ST and verified that “obtain time from the underlying virtualization system” is not selected. Therefore, this assurance activity is not applicable.
Verdict	NA

5.7.3.3 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. If the TOE supports obtaining time from the underlying VS, the evaluator shall verify the Guidance Documentation specifies any configuration steps necessary. If no configuration is necessary, no statement is necessary in the Guidance Documentation. If there is a delay between updates to the time on the VS and updating the time on the TOE, the evaluator shall ensure the Guidance Documentation informs the administrator of the maximum possible delay.
Evaluator Findings	The evaluator examined the section titled **6.10.6.2 Set-time** and **6.13.2.1.5 System Time Commands** in the AGD titled **Basic System Configuration Guide** to verify that it instructs the administrator how to set the time. Upon investigation, the evaluator found that the AGD states that: Use the set-time command to set the system date and time. The time entered should be accurate for the time zone configured for the system. The system will convert the local time to UTC before saving to the system clock which is always set to UTC. If SNTP or NTP is enabled (no shutdown), this command cannot be used. The settime command does not take into account any daylight saving offset if defined. CLI Syntax: admin set-time date time Example: admin# set-time 2010/09/24 14:10:00 The TOE is not a VS and it does not obtain time from the underlying VS. The AGD titled '**NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide',** sub-section **'Setting Time'** has the following note: **Setting Time** For CC-NDcPP compliance, time can be manually set. Ensure that NTP client has been disabled. To set the date and time, use the following commands:

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

5.7.4 FPT_TST_EXT.1.1

5.7.4.1 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 **FPT_TST_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that: The TOE executes the following power-on self-tests: • Software integrity test: For this test, when the CPM boots up, the bootloader calculates the HMAC-SHA256 authentication code of that software image from the storage and compares it with the known value stored in storage. If the value is not the same then it will give an error which is present on the console, and then the device will reboot. If the values of HMAC-SHA256 matches, then it successfully executes the software image. • AES Known Answer Test -The AES encryption and AES decryption algorithms are tested using test vectors. The results are compared against pre-computed results to ensure the algorithms are operating properly. • CMAC Known Answer Test - With this test, the CMAC authentication code is generated for a known message and respected key. Both are compared to the expected authentication code, if they match the test gets passed and if they do not the test get failed. The message is displayed on the console screen. • GCM Known Answer Test - In this test, A known plain-text is encrypted using AES-GCM with a known 256-bit key, and the computed cipher-text is compared to the expected cipher-text. If they match, then the computed cipher-text is decrypted using the same key, and the recovered plaintext is compared with the original known plain-text. If they do not match, the test fails. If they match, the test passes. • CCM Known Answer Test - In this test, the known plain text is encrypted using the AES-CCM with known 192 bits key, and then the computed cipher text is compared against the expected cipher txt . If they match, then the computed cipher-text is decrypted using the same key, and the recovered plaintext is compared with the original known plain-text. If they do not match, the test fails. If they match, the test passes.

	• HMAC-SHA-1/224/256/384/512 Known Answer Test - the HMAC algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • SHA-1/256/512 Known Answer Test - the SHA algorithm is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating correctly. • RSA Signature Known Answer Test - the RSA Signature is tested using test vector. The results are compared against pre-computed results to ensure the algorithm is operating properly. • DRBG Known Answer Test - the DRBG is seeded with a pre-determined entropy and the RNG output is compared with output values expected for the pre-determined seed. is also executed as part of self-tests. • The Software Integrity Test - is run automatically on start-up, and whenever the system images are loaded. These tests are sufficient to verify that the correct version of the TOE software is running as well as that the cryptographic operations are all performing as expected. • There is also a Noise Source Health test that is executed as part of the self-test requirements. The evaluator examined the **FPT_TST_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE executes the integrity check of the installed firmware by comparing the published HMAC-SHA256. If the hash does not match, the inactive CPM will reboot continuously until the CF is replaced with an authentic firmware. The TOE also performs self-tests for the cryptographic module during boot up, and if any component reports failure for the self-test, the system will reboot and display the appropriate information on the local console. All ports are blocked from moving to forwarding state during the POST. If all components of all modules pass the POST, the system is placed in FIPS PASS state and ports are allowed to forward data traffic. When any of the tests fail, a message is displayed to the local console. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.4.2 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 the section titled **5.1.3 FIPS-140-2 Mode** in the AGD titled **Basic System Configuration Guide** 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: To support the implementation of FIPS-140-2, the TiMOS software image contains an HMAC-SHA-256 secret key that is verified upon boot-up. When FIPS-140-2 is enabled on the node, an HMAC-SHA-256 integrity check is performed during the loading of the both.tim file to ensure that the calculated HMAC-SHA-256 secret key of the loaded image matches that stored in the hmac-sha256.txt file. This is a signature file that has been added to the TiMOS software image and only applies to FIPS-140-2. Note: The hmac-sha256.txt file must be stored in the same directory as the TiMOS image. If the image fails the HMAC-SHA-256 check, the node does not boot up, an error message is displayed, and the node tries to reboot the load after a delay of 60 s. The node keeps trying to reboot until the operator cancels the reboot. If the software image is verified by the HMAC-SHA-256 check, the node boots up normally and a message indicating that the software load has passed verification is displayed. The node performs its normal boot-up sequence, including reading the config.cfg file and loading the configuration. The config.cfg file that is used to boot the node in FIPS-140-2 mode must not contain any configuration that is not supported by the FIPS-140-2 implementation. If such a configuration is present in the config.cfg file when the node boots up, the node loads the config.cfg file until the unsupported configuration is reached and then stops. A failure message is also displayed. When the node boots in FIPS-140-2 mode, Cryptographic Module Validation Program (CMVP) startup tests are executed on the CSM and applicable data plane. CMVP conditional tests, such as manual key entry tests, pairwise consistency checks, and RNG tests, are executed when required during normal operation. In the CC guide titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide',** section '**Firmware Installation'** sub-section **'Issues that may affect successful boot of device/firmware'** has the following additional guidance statements for administrators to follow: **Issues that may affect successful boot of device/ firmware** There may be instances where the device ends up not booting correctly. It can be a result of firmware failure, a POST test failure, or other things. The administrators are advised to refer to the available official administrative guidance documents to look for solution and if the issues are not resolved, contact Nokia support. Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.7.5 FPT_TUD_EXT.1

5.7.5.1 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 **FPT_TUD_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target to verify that the TSS describes how to query the currently active version. Upon investigation, the evaluator found that the TSS states that: The TOE implements a "show version" CLI command for the Security Administrators to query the current version of the TOE software. The administrators may also perform manual software updates. The TOE does not implement functions for automatically upgrading the software, each upgrade must be performed manually by the Administrator. The TOE does not support delayed activation. The uploading of the TOE firmware and selection of the boot image are a manual process. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.2 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 **FPT_TUD_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that:

	To upgrade the TOE software, the Administrator first connects to the update server using FTP or SFTP and downloads the firmware upgrade to a Compact Flash (CF) device. The upgrade is protected by a HMAC-SHA-256 value which is computed by the developer in the development environment and stored in a separate file. The TOE uses a Boot Options File (BOF) for indicating to the boot loader the location of the TOE software. Typically, the Administrator stores the firmware upgrade on a CF and modifies the BOF to point to the software on the CF. This does not need to be performed immediately after downloading the software upgrade. The Administrator may time the actual upgrading at a convenient time. When rebooting the TOE with the modified BOF, the TOE upgrades the software from the source pointed to by the BOF. When in the FIPS mode, the boot loader searches for the hash file containing the HMAC-SHA-256 value of the TOE software in the same location as the software image. When the HMAC file is found, the TOE computes a HMAC value of the image and compares it to the value on the HMAC file. If the values match, the TOE continues with the boot up. If the HMAC file is not found or the comparison fails, the boot loader reboots the system. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.3 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 Security Target and found that the options 'support automatic checking for updates' or 'support automatic updates' are not chosen from the selection in FPT_TUD_EXT.1.2. Based on these findings, this assurance activity is considered NA.
Verdict	NA

5.7.5.4 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 **FPT_TUD_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: To upgrade the TOE software, the Administrator first connects to the update server using SFTP and downloads the firmware upgrade to a Compact Flash (CF) device. The upgrade is protected by a HMAC-SHA-256 value which is computed by the developer in the development environment and stored in a separate file. The TOE uses a Boot Options File (BOF) for indicating to the boot loader the location of the TOE software. Typically, the Administrator stores the firmware upgrade on a CF and modifies the BOF to point to the software on the CF. This does not need to be performed immediately after downloading the software upgrade. The Administrator may time the actual upgrading at a convenient time. When rebooting the TOE with the modified BOF, the TOE upgrades the software from the source pointed to by the BOF. When in the FIPS mode, the boot loader searches for the hash file containing the HMAC-SHA-256 value of the TOE software in the same location as the software image. When the HMAC file is found, the TOE computes a HMAC value of the image and compares it to the value on the HMAC file. If the values match, the TOE continues with the boot up. If the HMAC file is not found or the comparison fails, the boot loader reboots the system. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.5 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 the section titled **3.8.5 History** and **4.3.2.1 Configuration Commands** in the AGD titled **Basic System Configuration Guide** 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: **3.8.5 History** *A:ALU-1# show version TiMOS-B-0.0.I322 both/hops NOKIA SAR 7705 Copyright (c) 2018 Nokia.All rights reserved. All use subject to applicable license agreements.

	Built on Wed Jan 17 01:05:13 EST 2018 by csabuild in /re8.0/I322/panos/main *A:ALU-1# **4.3.2.1 Configuration Commands** version Syntax version file-url [check] Context file Description This command displays the version of a TiMOS both.tim file. Parameters file-url — the filename of the target file (see Table 15 for parameter descriptions) check — validates the .tim file Output The following example shows the version of a TiMOS both.tim file. The TOE does not support delayed activation. The uploading of the TOE firmware and selection of the boot image are a manual process. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.6 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 the section titled **5.1.3 FIPS-140-2 Mode** in the AGD titled **Basic System Configuration Guide** 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: To upgrade the TOE software, the Administrator first connects to the update server using FTP or SFTP and downloads the firmware upgrade to a Compact Flash (CF) device. The upgrade is protected by a HMAC-SHA-256 value which is computed by the developer in the development environment and stored in a separate file. The TOE uses a Boot Options File (BOF) for indicating to the boot loader the location of the TOE software. Typically, the Administrator stores the firmware upgrade on a CF and modifies the BOF to point to the software on the CF. This does not need to be performed immediately after downloading the software upgrade. The Administrator may time the actual upgrading at a convenient time.

	When rebooting the TOE with the modified BOF, the TOE upgrades the software from the source pointed to by the BOF. When in the FIPS mode, the boot loader searches for the hash file containing the HMAC-SHA-256 value of the TOE software in the same location as the software image. When the HMAC file is found, the TOE computes a HMAC value of the image and compares it to the value on the HMAC file. If the values match, the TOE continues withthe boot up. If the HMAC file is not found or the comparison fails, the boot loader reboots the system. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.7.5.7 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 the section titled **5.1.3 FIPS-140-2 Mode** in the AGD titled **Basic System Configuration Guide** 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: To upgrade the TOE software, the Administrator first connects to the update server using SFTP and downloads the firmware upgrade to a Compact Flash (CF) device. The upgrade is protected by a HMAC-SHA-256 value which is computed by the developer in the development environment and stored in a separate file. The TOE uses a Boot Options File (BOF) for indicating to the boot loader the location of the TOE software. Typically, the Administrator stores the firmware upgrade on a CF and modifies the BOF to point to the software on the CF. This does not need to be performed immediately after downloading the software upgrade. The Administrator may time the actual upgrading at a convenient time. When rebooting the TOE with the modified BOF, the TOE upgrades the software from the source pointed to by the BOF. When in the FIPS mode, the boot loader searches for the hash file containing the HMAC-SHA-256 value of the TOE software in the same location as the software image. When the HMAC file is found, the TOE computes a HMAC value of the image and compares it to the value on the HMAC file. If the values match, the TOE continues withthe boot up. If the HMAC file is not found or the comparison fails, the boot loader reboots the system. The same information can be found in the CC guide titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'.** Based on these findings, this assurance activity is considered satisfied.

Verdict	Pass

5.7.5.8 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 the Security Target and verified that a certificate-based mechanism is not used for software update digital signature verification. Based on these findings, this assurance activity is considered NA.
Verdict	NA

5.8 TSS and Guidance Activities (TOE Access)

5.8.1 FTA_SSL_EXT.1

5.8.1.1 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 **FTA_SSL_EXT.1** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE will terminate a remote interactive session after a configurable time interval of session inactivity. A configured inactivity period will be applied to both local and remote sessions in the same procedure. When the interface has been idle for more than the configured period, the session will be terminated and will require authentication to establish a new session. If a local user session is not active for a configured period of time, the session will be terminated and will require re-identification and authentication to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require re-identification and authentication to establish a new session. When the user logs back in, the inactivity timer will be activated for the new session. A configured inactivity period will be applied to both local and remote sessions in the same manner. The allowable inactivity timeout range is from 1 to 1440 minutes.

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

5.8.1.2 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 the section titled **3.10.2.1.6 Password Commands** in the AGD titled **System Management Guide** 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: attempts Syntax attempts count [time minutes1] [lockout minutes2] no attempts Context config>system>security>password Description This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame. If the threshold is exceeded, the user is locked out for a specified time period. If multiple attempts commands are entered, each command overwrites the previously entered command. The no attempts command resets all values to the default. Default count: 3 minutes1: 5 minutes2: 10 Parameters count — the number of unsuccessful login attempts allowed for the specified time. This is a mandatory value that must be explicitly entered. Values 1 to 64 minutes1 — the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out

	Values 0 to 60 minutes2 — the lockout period, in minutes, where the user is not allowed to log in Values 0 to 1440 When the user exceeds the attempted count times in the specified time, then that user is locked out from any further login attempts for the configured time period. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2 FTA_SSL.3

5.8.2.1 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 **FTA_SSL_EXT.3** entry in the section titled **TOE Summary Specification** in the Security Target 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: The TOE will terminate a remote interactive session after a configurable time interval of session inactivity. A configured inactivity period will be applied to both local and remote sessions in the same procedure. When the interface has been idle for more than the configured period, the session will be terminated and will require authentication to establish a new session. If a local user session is not active for a configured period of time, the session will be terminated and will require re-identification and authentication to establish a new session. If a remote user session is inactive for a configured period of time, the session will be terminated and will require re-identification and authentication to establish a new session. When the user logs back in, the inactivity timer will be activated for the new session. A configured inactivity period will be applied to both local and remote sessions in the same manner. The allowable inactivity timeout range is from 1 to 1440 minutes. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.2.2 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 the section titled **3.10.2.1.6 Password Commands** in the AGD titled **System Management Guide** 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 states that: attempts Syntax attempts count [time minutes1] [lockout minutes2] no attempts Context config>system>security>password Description This command configures a threshold value of unsuccessful login attempts allowed in a specified time frame. If the threshold is exceeded, the user is locked out for a specified time period. If multiple attempts commands are entered, each command overwrites the previously entered command. The no attempts command resets all values to the default. Default count: 3 minutes1: 5 minutes2: 10 Parameters count — the number of unsuccessful login attempts allowed for the specified time. This is a mandatory value that must be explicitly entered. Values 1 to 64 minutes1 — the period of time, in minutes, that a specified number of unsuccessful attempts can be made before the user is locked out Values 0 to 60 minutes2 — the lockout period, in minutes, where the user is not allowed to log in

	Values 0 to 1440 When the user exceeds the attempted count times in the specified time, then that user is locked out from any further login attempts for the configured time period. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3 FTA_SSL.4

5.8.3.1 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 **FTA_SSL_EXT.4** entry in the section titled **TOE Summary Specification** in the Security Target 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 manually terminate their CLI using the command 'logout'. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.3.2 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 the section titled **3.11.2.1 Basic CLI Commands** in the AGD titled **Basic System Configuration Guide** to verify that it states how to terminate a local or remote interactive session. Upon investigation, the evaluator found that the AGD states that: logout Syntax logout Context <global> Description This command logs out of the router session. When the logout command is issued from the console, the login prompt is displayed and any log IDs directed to the console are discarded. When the console session resumes (regardless of the user), the log output to the console resumes.

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

5.8.4 FTA_TAB.1

5.8.4.1 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 **FTA_TAB.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 states that: Security Administrators can create a customized login banner that will be displayed at the following interfaces: • Local CLI • Remote CLI This banner will be displayed prior to allowing Security Administrator access through those interfaces. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.8.4.2 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 the section titled **3.10.2.1.15 Login Control Commands** in the AGD titled **System Management Guide** to verify that it describes how to configure the banner message. Upon investigation, the evaluator found that the AGD states that: pre-login-message Syntax pre-login-message login-text-string [name]

	no pre-login-message Context config>system>login-control Description This command creates a message displayed prior to console login attempts on the console via Telnet. Only one message can be configured. If multiple pre-login messages are configured, the last message entered overwrites the previous entry. The system name can be added to an existing message without affecting the current pre-login message. The no form of the command removes the message. Default no pre-login-message Parameters login-text-string — a text string, up to 900 characters. Any printable, 7-bit ASCII characters can be used. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. name — when the keyword name is defined, the configured system name is always displayed first in the login message. To remove the name from the login message, the message must be cleared and a new message entered without the name. login-banner Syntax [no] login-banner Context config>system>login-control Description This command enables or disables the display of a login banner. The login banner contains the 7705 SAR copyright and build date information for a console login attempt. The no form of the command causes only the configured pre-login-message and a generic login prompt to display. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9 TSS and Guidance Activities (Trusted Path/Channels)

5.9.1 FTP_ITC.1

5.9.1.1 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 **FTP_ITC.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 supports secure communication to the following IT entities: Audit server and Authentication server. The TOE provides secure communication by using IPSEC between itself and Audit server, and between itself and Authentication server. The TOE uses IPSEC protocol with X.509 certificate-based authentication. The protocols listed are consistent with those specified in the requirement. The evaluator examined the **FTP_ITC.1** entry in the section titled **TOE Summary Specification** in the Security Target 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 provides secure communication by using IPSEC between itself and Audit server, and between itself and Authentication server. The TOE uses IPSEC protocol with X.509 certificate-based authentication. The protocols listed are consistent with those specified in the requirement. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.1.2 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 the section titled **'Using a Secure Audit Server',** sub-section **'Configure TOE to communicate with an Audit Server'** and the section titled **'Authentication',** sub-sections **'Authentication using RADIUS Server' & 'Authentication using TACACS+**

	Server' in the AGD titled **'NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'** 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 states that: **<u>Using IPSec tunnelling to secure communication between the device and the Audit Server.</u>** • If an authorized administrator wants to back up logs to a syslog server, then protection must be provided for the syslog server communications which can be done with a syslog server operating as an IPsec peer of the TOE and the log records being tunneled over that connection. • If the IPsec connections used by the TOE is unintentionally broken, the security administrator needs to restart the connection, or the TOE will try to re-connect with the audit server. • When a Syslog server is configured on the TOE, the generated audit events are simultaneously sent to the external server and the local logging buffer. **<u>Using IPSec tunnelling to secure communication between the device and the RADIUS Server.</u>** • The communication between the RADIUS Server and the Nokia SAR devices must be protected by using IPSec tunnels. IPSec tunnel configuration steps can be found in section 7.2 below. • If the IPsec connections used by the Nokia SAR 7705 device is unintentionally broken, the security administrator needs to restart the connection, or the device will try to re-connect with the authentication server. **<u>Using IPSec tunnelling to secure communication between the device and the TACACS+ Server.</u>** • The communication between the TACACS+ Server and the Nokia SAR devices must be protected by using IPSec tunnels. IPSec tunnel configuration steps can be found in section 7.2 below. • If the IPsec connections used by the Nokia SAR 7705 device is unintentionally broken, the security administrator needs to restart the connection, or the device will try to re-connect with the authentication server. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2 FTP_TRP.1/Admin

5.9.2.1 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 **FTP_TRP.1/Admin** entry in the section titled **TOE Summary Specification** in the Security Target 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 SSH v2.0 for secure remote administration of the TOE. SSH v2.0 session is encrypted using AES encryption to protect confidentiality and uses HMACs to protect integrity of traffic. The protocols listed are consistent with those specified in the requirement. Next, the evaluator compared the protocols identified in the TSS to the definition of the SFR. The evaluator found that the protocols listed in the TSS are consistent with the protocols listed in the definition of the SFR. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

5.9.2.2 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 the section titled **3.10.1.1.13 SSH Commands** in the AGD titled **System Management Guide** and to verify that it contains instructions for establishing the remote administrative sessions for each supported method. Upon investigation, the evaluator found that the AGD states that: In particular, the evaluator found that these instructions include configuration of the protocols used to secure remote administrative session. Specifically, each AGD provides instructions for configuring the following protocols: SSH. Based on these findings, this assurance activity is considered satisfied.
Verdict	Pass

6 Detailed Test Cases (Test Activities)

6.1 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	• The audit records required for this test case can be found in the test cases associated with each of the listed SFRs.
Expected Test Results	• The TOE should be able to generate audit records for establishment and termination of a channel for each of the listed SFRs. • The audit records generated should match the proper format as specified in the guidance documentation.
Pass/Fail with Explanation	Pass, covered by audit records in each test case. This meets the testing requirements.

6.2 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.
Pass/Fail with Explanation	Pass. This test case has been covered by the requirements in FTP_ITC.1 Test #1.

6.3 FAU_STG_EXT.1 Test #2 (a)

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 audit data remains unchanged with every new auditable event that should be tracked but that the audit data is recorded again after the local storage for audit data is cleared (for the option '**drop new audit data**' in FAU_STG_EXT.1.3).
Pass/Fail with Explanation	NA. The ST does not select '**drop new audit data**'.

6.4 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	• Display the configuration of the log. • Generate audit data. • Verify the oldest audit record stored locally. • Generate audit data. • Verify that the oldest audit record stored locally is no longer available.
Expected Test Results	Evidence (screenshot) showing that the TOE overwrites the oldest log file when the local audit space is filled.
Pass/Fail with Explanation	Pass. The evaluator has verified that TOE generates audit data and verified that this data is stored locally. The evaluator has also verified that the TOE overwrites previous audit records when the local storage space is exceeded.

6.5 FAU_STG_EXT.1 Test #2 (c)

Item	Data
Test Assurance Activity	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 TOE behaves as specified (for the option '**other action**' in FAU_STG_EXT.1.3).
Pass/Fail with Explanation	NA. The ST does not select '**other action**'.

6.6 FAU_STG_EXT.1 Test #4

Item	Data
Test Assurance Activity	Test 4: For distributed TOEs, Test 1 defined above should be applicable to all TOE components that forward audit data to an external audit server. For the local storage according to FAU_STG_EXT.1.2 and FAU_STG_EXT.1.3 the Test 2 specified above shall be applied to all TOE components that store audit data locally. For all TOE components that store audit data locally and comply with FAU_STG_EXT.2/LocSpace Test 3 specified above shall be applied. The evaluator shall verify that the transfer of audit data to an external audit server is implemented.
Pass/Fail with Explanation	This test is not applicable since the TOE is not a distributed TOE

6.7 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	• Confirm the current time on the TOE. • Set a new time on the TOE. • Verify that the new time is set. • Verify that the new time is set via log.
Expected Test Results	• Evidence (screenshots, logs) showing that the time was set correctly as per the guidance document.
Pass/Fail with Explanation	Pass. The evaluator has verified that administrator can set the time on the TOE.

6.8 FPT_STM_EXT.1 Test #2

Item	Data
Test Assurance Activity	Test 2: If the TOE supports the **use of an NTP server**; the evaluator shall use the guidance documentation to configure the NTP client on the TOE, and set up a communication path with the NTP server. The evaluator will observe that the NTP server has set the time

	to what is expected. If the TOE supports multiple protocols for establishing a connection with the NTP server, the evaluator shall perform this test using each supported protocol claimed in the guidance documentation.
Pass/Fail with Explanation	NA. The ST does not select '**use of an NTP server**'.

6.9 FPT_STM_EXT.1 Test #3

Item	Data
Test Assurance Activity	If **the audit component of the TOE consists of several parts with independent time information**, then the evaluator shall verify that the time information between the different parts are either synchronized or that it is possible for all audit information to relate the time information of the different part to one base information unambiguously.
Pass/Fail with Explanation	NA. The ST does not select '**the audit component of the TOE consists of several parts with independent time information**'.

6.10 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	**<u>Syslog over IPsec</u>** • Identify the audit software (name and version) used for this test. • Verify the status of the Syslog server. • Configure the TOE to communicate with an audit server. • Establish the IPsec tunnel. • Generate audit events. • Verify that audit the logs have been transferred to audit server. • Verify that the logs match with the logs on the audit server. • Verify via packet capture that the traffic between the TOE and an audit server is not sent in plaintext. **<u>Authentication using Radius Server</u>** • Identify the name and version of the Radius server along with the status used for this test. • Configure the TOE to communicate with the Radius server.

	• Configure the Radius Server on the VM. • Establish the IPsec tunnel. • Authenticate the user in the Radius server. • Verify via logs that the user was authenticated. Verify that the connection was established successfully via packet capture and the traffic is encrypted.
Expected Test Results	• Evidence (Screenshots, packet capture) showing that communications using each protocol with the TOE is tested. Evidence (Screenshots, packet capture) showing that the TOE is able to initiate connection to an external audit server & Authentication server and the traffic is not sent in plaintext.
Pass/Fail with Explanation	Pass. The TOE can be configured to successfully communicate with the external authentication server and syslog server via IPsec.

6.11 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.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FCS_IPsec_EXT.1.1 Test #1.

6.12 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.
Pass/Fail with Explanation	Pass. This testing was performed in conjunction with FCS_IPsec_EXT.1.1 Test #1.

6.13 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	**Syslog over IPsec** **A duration shorter than the application layer timeout but of sufficient length to interrupt the network link layer - 2 minutes** • Configure the TOE. • Configure dead-peer-detection on the TOE. • Establish the IPsec tunnel. • Send traffic through the IPsec tunnel. • Interrupt the connection between the TOE and peer for a duration that is shorter than the application layer timeout but of sufficient length to interrupt the MAC layer (2 minutes) and verify that connection is down. **A duration that exceeds the application layer timeout but is of sufficient length to interrupt the network link layer - 10 minutes** • Establish the IPsec tunnel. • Generate Audit logs. • Interrupt the connection between the TOE and peer for a duration that exceeds the application layer timeout but of sufficient length to interrupt the MAC layer (10 minutes) and verify that connection is down.
Expected Test Results	Evidence (screenshot, packet capture) showing that the data exchanged between both audit server & auth Server is encrypted after the physical connectivity with a remote audit server & auth Server is interrupted and then restored
Pass/Fail with Explanation	Pass. When physical connectivity with a syslog and IPX server is interrupted and then restored, the data is exchanged between both entities is never in plaintext, as can be shown by packet captures during and after the outage. This meets the testing requirement.

6.14 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.

Pass/Fail with Explanation	Pass. This testing will be performed in conjunction with FTP_TRP.1/Admin_T1 and FTP_ITC.1 Test 1 to demonstrate correct operation. This meets the testing requirements.

6.15 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	• Configure the TOE to have only certain number of attempts for authentication. • Attempt to connect to the TOE with incorrect credentials till the TOE locks out. • Verify to connect with right credential and the attempt should fail. Verify with the logs that user with incorrect credentials has been locked after reaching the number of successive unsuccessful authentication attempts.
Expected Test Results	• Evidence (screenshot) of the TOE settings showing that 3 successive unsuccessful login attempts were configured. • Evidence (screenshot, logs) of the evaluator attempting to login with incorrect credentials. • Evidence (screenshot, logs) of the evaluator attempting to login with correct credentials. Evidence (screenshot, logs) showing that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful.
Pass/Fail with Explanation	Pass. The evaluator has verified that once the authentication attempts limit is reached, authentication attempts with valid credentials are no longer successful. This meets the testing requirements.

6.16 FIA_AFL.1 Test #2a

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 fs 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).

Pass/Fail with Explanation	NA. The ST does not select '**administrator action**'.

6.17 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 **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 period configured in Test 1 and show that an authorisation attempt using valid credentials results in successful access.
Test Steps	• Attempt to connect to the TOE from an SSH client using incorrect credentials until the lockout threshold has been met. • Wait till a time period which is slightly less than the configured lockout threshold and verify that the login attempt fails. • Wait till a time period which is slightly longer than the configured lockout threshold and attempt to log into the TOE using correct credentials. Verify via logs that the login attempt with correct credentials succeeds.
Expected Test Results	• Evidence (screenshot) of the connection showing that 3 failed login attempts were configured. • Evidence (screenshot, logs) showing that connection is closed after 3 failed login attempts. • Evidence (screenshot, logs) showing that the attempt to login fails if the time period is slightly less than the configured lockout threshold. Evidence (screenshot, logs) showing that the attempt to login succeeds if the time period is slightly longer than the configured lockout threshold.
Pass/Fail with Explanation	Pass. The evaluator has verified that TOE didn't allow to log in successfully until the time period configured in FIA_AFL.1 Test #1 has been met and verified that an authorization attempt using valid credentials results in successful access after the threshold limit. This meets the testing requirements.

6.18 FIA_PMG_EXT.1.1 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	• Configure the TOE to require a minimum of 6-character passwords. • Configure a user with a required password comprised of all letters (non-repeating). • Configure a user with a required password comprised of all numbers (may be repeating). • Configure a user with a required password comprised of at least the following “!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)” • Configure a user with a 20-character password comprised of any set of characters. • Configure a user with a 30-character password comprised of any set of characters. • Verify that a log was generated for each creation.
Expected Test Results	• Evidence (screenshot) of the evaluator attempting to create a password with minimum length 6. • Evidence (screenshot) of the evaluator attempting to create a password comprised of all letters that are non-repeating. • Evidence (screenshot) of the evaluator attempting to create a password comprised of all numbers that may be repeating. • Evidence (screenshot) of the evaluator attempting to create a password comprised of all the special characters documented in the ST. • Evidence (screenshot) of the evaluator attempting to create a 20-character password comprised of any set of characters. Evidence (screenshot) of the evaluator attempting to create a 30-character password comprised of any set of characters.
Pass/Fail with Explanation	Pass. The evaluator has verified that the TOE supports the passwords which have all the characters and a minimum length listed in the requirement and justified the subset of those passwords. This meets the testing requirements.

6.19 FIA_PMG_EXT.1.1 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	• Configure the TOE to require a minimum of 6-character passwords. • Configure a user with a 1-character password. • Configure a user with a 5-character password. • Configure a user with a password one more character than the maximum 60 allowed characters. Verify that each attempt fails, and a log was generated for each attempt.
Expected Test Results	Evidence (screenshot) showing that the TOE does not support the passwords which do not meet the minimum length requirement and other requirements.
Pass/Fail with Explanation	Pass, the TOE rejects user creation with bad passwords. This meets the testing requirements.

6.20 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	**Password-based:** • Attempt to login from a local connection with incorrect credentials. • Confirm that the access was denied. • Verify that an audit record was generated for the authentication attempt. • Log into the TOE from a local connection with correct credentials. • Confirm that access was granted. • Verify that an audit record was generated for the authentication. • Attempt to login from a remote CLI connection through SSH with incorrect credentials. • Confirm that the access was denied. • Verify that an audit record was generated for the authentication attempt. • Log into the TOE from a remote CLI connection through SSH with correct credentials. • Confirm that access was granted. • Verify that an audit record was generated for the authentication. **SSH Public Key-based:** • Create a new key pair on the client. • Import this public key onto the TOE and verify that it is updated on the TOE. • Attempt to authenticate the client through SSH and verify that the login is successful. • Verify via logs that the attempt was successful. • Create a new pair key on the client and do not import it on the TOE. • Attempt to authenticate the client through SSH and verify that the login is unsuccessful. • Verify via logs that the attempt was unsuccessful.

	Authentication using Radius Server: • Configure the radius server on the TOE. • Configure the radius server on the VM. • Log into the TOE from a remote CLI connection through SSH with correct credentials via Radius Server. • Verify that an audit record was generated for the authentication. • Verify that the authentication was successful via packet capture. • Log into the TOE from a remote CLI connection through SSH with incorrect credentials via RADIUS server and verify that the access was rejected. • Verify that an audit record was generated for the authentication. • Verify that the connection could not be established using packet capture. **Authentication using TACACS Server:** • Configure the TACACS server on the TOE. • Configure the TACACS server on the VM. • Log into the TOE from a remote CLI connection through SSH with correct credentials via TACACS Server. • Verify that an audit record was generated for the authentication. • Verify that the authentication was successful via packet capture. • Log into the TOE from a remote CLI connection through SSH with incorrect credentials via TACACS server and verify that the access was rejected. • Verify that an audit record was generated for the authentication. • Verify that the connection could not be established using packet capture.
Expected Test Results	• Evidence (screenshot) showing that providing correct I&A information results in the ability to access the system, while providing incorrect information results in denial of access. • Evidence (screenshot) showing that the TOE only grants access when it is provided correct credentials and the TOE denies access when the user provides incorrect credentials for both password-based and SSH public key-based authentication methods.
Pass/Fail with Explanation	Pass. It has been verified that the TOE only grants access when it is provided correct credentials and the TOE denies access when the user provides incorrect credentials for both password-based and SSH public key-based authentication methods. This meets the testing requirements.

6.21 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	**<u>Password-based:</u>** • Verify that only the login banner was displayed while attempting to log into the TOE. **<u>Authentication using Radius Server.</u>** • Verify that only the login banner is visible while attempting to log into the TOE using the Radius server user “test”. **<u>Authentication using TACACS Server.</u>** Verify that only the login banner is visible while attempting to log into the TOE using the TACACS server user “user176”.
Expected Test Results	• Evidence (Screenshot) showing that the list of services available is limited to those specified in the requirement. Evidence (Screenshot) showing that only the login banner was displayed while attempting to log into the TOE.
Pass/Fail with Explanation	Pass. No system services are available to an unauthenticated user connecting remotely except for the banner. This meets the testing requirements.

6.22 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	• Show that commands are not available prior to login. • Verify authentication logs reflect failure. • Verify that only the login banner was displayed. • Login into the TOE. • Show that the previously entered commands are now available. • Verify authentication logs reflect success.

Expected Test Results	• Evidence (Screenshot) showing that the list of services available to a local administrator prior to logging in is limited to those specified in the requirement. • Evidence (Screenshot) showing that the commands which were not available prior to login are available after logging into the TOE.
Pass/Fail with Explanation	Pass. No system services are available to an unauthenticated user connecting via local CLI except for the banner. This meets the testing requirements.

6.23 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	• At the directly connected login prompt, enter incorrect authentication credentials. • Verify that at most obscured feedback is provided. • At the directly connected login prompt, enter correct authentication credentials. • Verify that at most obscured feedback is provided.
Expected Test Results	• Evidence (Screenshots) showing that the TOE provides obscured feedback when incorrect credentials are entered. • Evidence (Screenshots) showing that the TOE provides no feedback when correct credentials are entered.
Pass/Fail with Explanation	Pass. The evaluator has verified that at most obscured feedback is provided while entering the authentication information. This meets the testing requirements.

6.24 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	• At the command prompt, log into the TOE as a user with no administrative privileges. • Verify that the user “sarx” does not have administrative privileges by comparing it with user “admin” which has administrative privileges. • From the unauthenticated command prompt, attempt to execute the commands associated with performing an image update. • Verify the attempt is unsuccessful.

Expected Test Results	- Evidence (Screenshots) showing that when an unprivileged account tries to update a legitimate image, it results in failure as the user doesn't have the administrator privilege. Evidence (Screenshots) showing that the user "sarx" does not have administrative privileges.
Pass/Fail with Explanation	Pass. The evaluator has attempted the update using a legitimate update image authentication as a user with no administrator privileges and verified that update the TOE was failed. This meets the testing requirements.

6.25 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.
Pass/Fail with Explanation	This test has been covered by FPT_TUD_EXT.1 test #1

6.26 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	- Connect to the TOE as an unprivileged user. - Attempt 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 and verify that this attempt fails. - Attempt to modify the parameters involved with the syslog server. - Verify that the TOE rejected the modification.
Expected Test Results	- Evidence (screenshots) showing that an attempt to modify the 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 fails. - Evidence (screenshots) showing that an attempt to modify the parameters involved with the syslog server without prior authentication as Security Administrator fails.

Pass/Fail with Explanation	Pass. It has been verified that when an unprivileged user tries to modify the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity, this attempt fails.

6.27 FMT_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	• Log into the TOE as an administrator. • Attempt 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 and verify that this attempt is successful. • Attempt to modify the parameters involved with the syslog server. • Verify that the modifications are successful.
Expected Test Results	• Evidence (screenshots) showing that an attempt to modify the security related parameters for configuration of the transmission protocol for transmission of audit data to an external IT entity with authentication as a Security Administrator is successful. • Evidence (screenshots) showing that an attempt to modify the parameters involved with the syslog server with authentication as a Security Administrator is successful.
Pass/Fail with Explanation	Pass. It has been verified that when a privileged user tries to modify the security related parameters for configuration of the transmission protocol (IPsec) for transmission of audit data to an external IT entity, this attempt is successful.

6.28 FMT_MOF.1/Functions (2) Test #1

Item	Data
Test Assurance Activity	(Test 1 (if **'handling of audit data'** 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 handling of audit data 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 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. The term ‘handling of audit data’ refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace.
Pass/Fail with Explanation	NA. The ST does not select **'handling of audit data'.**

6.29 FMT_MOF.1/Functions (2) Test #2

Item	**Data**
Test Assurance Activity	(if **'handling of audit data'** 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 handling of audit data with prior authentication as Security Administrator. The effects of the modifications should be confirmed. The term ‘handling of audit data’ refers to the different options for selection and assignments in SFRs FAU_STG_EXT.1.2, FAU_STG_EXT.1.3 and FAU_STG_EXT.2/LocSpace. The evaluator does not necessarily have to test all possible values of the security related parameters for configuration of the handling of audit data but at least one allowed value per parameter.
Pass/Fail with Explanation	NA. The ST does not select **'handling of audit data'.**

6.30 FMT_MOF.1/Functions (3) Test #1

Item	**Data**
Test Assurance Activity	(if **'audit functionality when Local Audit Storage Space is full'** is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This attempt 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 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.
Pass/Fail with Explanation	NA. The ST does not select '**audit functionality when Local Audit Storage Space is full**'.

6.31 FMT_MOF.1/Functions (3) Test #2

Item	Data
Test Assurance Activity	(if **'audit functionality when Local Audit Storage Space is full'** is selected from the second selection together with 'modify the behaviour of' in the first selection): The evaluator shall try to modify the behaviour when Local Audit Storage Space is full with prior authentication as Security Administrator. This attempt should be successful. The effect of the change shall be verified. The evaluator does not necessarily have to test all possible values for the behaviour when Local Audit Storage Space is full but at least one change between allowed values for the behaviour
Pass/Fail with Explanation	NA. The ST does not select **'audit functionality when Local Audit Storage Space is full'**.

6.32 FMT_MOF.1/Functions Test #3

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection without prior authentication as Security Administrator (by authentication as a user with no administrator privileges or without user authentication at all). This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions without administrator authentication shall 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 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.
Pass/Fail with Explanation	NA. The ST does not select **'determine the behaviour of'**.

6.33 FMT_MOF.1/Functions Test #4

Item	Data
Test Assurance Activity	(if in the first selection **'determine the behaviour of'** has been chosen together with for any of the options in the second selection): The evaluator shall try to determine the behaviour of all options chosen from the second selection with prior authentication as Security Administrator. This can be done in one test or in separate tests. The attempt(s) to determine the behaviour of the selected functions with Security Administrator authentication shall be successful.
Pass/Fail with Explanation	NA. The ST does not select **'determine the behaviour of'**.

6.34 FMT_MOF.1/Services Test #1

Item	Data
Test Assurance Activity	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) without prior authentication as Security Administrator (either by authenticating as a user with no administrator privileges, if possible, or without prior authentication at all). The attempt to enable/disable this service/these services 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 enable/disable this service/these services 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	• Login with a non-administrator account. • Attempt to configure the parameters of user 'test1'. • Show that the TOE rejects the modifications.
Expected Test Results	• Evidence (Screenshots) showing that the TOE rejects the modifications attempted for user 'test1' using a non-administrator account.
Pass/Fail with Explanation	Pass. The TOE did not allow to configure the parameters of user 'test1' when logged in as non admin user. This meets the testing requirements.

6.35 FMT_MOF.1/Services Test #2

Item	Data
Test Assurance Activity	The evaluator shall try to enable and disable at least one of the services as defined in the Application Notes for FAU_GEN.1.1 (whichever is supported by the TOE) with prior authentication as Security Administrator. The attempt to enable/disable this service/these services should be successful.
Test Steps	• Login with an administrator account. • Attempt to configure the parameters of user 'test1'.

	- Show that the TOE allows the modifications.
Expected Test Results	- Evidence (Screenshots) showing that the TOE allows the modifications attempted for user 'test1' using an administrator account.
Pass/Fail with Explanation	Pass. The TOE allows to configure the parameters of user 'test1' when logged in as an admin user. This meets the testing requirements.

6.36 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	- Login with a non-administrator account. - Verify that the user "sarx" does not have administrative privileges by comparing it with user "admin" which has administrative privileges. - Attempt to delete the public key of user 'test'. - Show that the TOE rejects the modifications.
Expected Test Results	- Evidence (screenshots) showing that the TOE does not allow to configure the parameters of user 'test1' when logged in as a non admin user. - Evidence (screenshots) showing that the user "sarx" has non-administrative privileges. - Evidence showing (screenshots) that the TOE does not allow to delete the public key of the user 'test'.
Pass/Fail with Explanation	Pass. The TOE did not allow to configure the parameters of user 'test' when logged in as non admin user. This meets the testing requirements.

6.37 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	- Login with an administrator account. - Verify that the user "admin" has administrative privileges.

	• Attempt to delete the public key of user 'test'. • Show that the TOE allows the modifications.
Expected Test Results	• Evidence showing (screenshots) that the TOE allows to configure the parameters of the user 'test' when logged in as an admin user. • Evidence (screenshots) showing that the user "admin" has administrative privileges. • Evidence showing (screenshots) that the TOE allows to delete the public key of the user 'test'.
Pass/Fail with Explanation	Pass. The TOE allowed to configure the parameters of user 'test' when logged in as an admin user. This meets the testing requirements.

6.38 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	All management functions identified in section 2.4.4 should be tested throughout the evaluation.
Expected Test Results	All management functions identified in section 2.4.4 should be tested throughout the evaluation.
Pass/Fail with Explanation	Pass. All management functions identified in section 2.4.4 have been tested throughout the evaluation. Thus, this requirement has been met.

6.39 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	The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces.
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. There are two interfaces (over the CLI/Console) used for testing and all test cases are tested that way. The evaluator has met this requirement through execution of the entirety of this test report for the TOE interfaces. This meets the testing requirements.

6.40 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	• Configure a remote CLI time out period of 1 minute for administrative sessions. • Connect to the TOE from the remote CLI. • Verify the time. • Let the remote CLI connection set idle for 1 minute and verify that the session was terminated. • Verify via log that user has been logged out. • Configure a remote CLI out period of 2 minutes for administrative sessions. • Connect to the TOE from the remote CLI. • Verify the time. • Let the remote CLI connection set idle for 2 minutes and verify that the session was terminated. • Verify via log that user has been logged out.
Expected Test Results	• Evidence showing (screenshots, logs) that for each period configured, the evaluator established remote interactive session with the TOE and then the evaluator observed that the session was terminated after the configured time period. • Evidence (screenshot) of the TOE being configured for 1 minute of remote session idle time. • Evidence (screenshot) of the evaluator verifying the current time on the TOE. • Evidence (screenshot) of TOE's remote session ending when waiting past the timeout expiration. • Evidence (screenshot, logs) of the TOE generating logs for all these events. • Evidence (screenshot) of the TOE being configured for 2 minutes of remote session idle time. • Evidence (screenshot) of the evaluator verifying the current time on the TOE. • Evidence (screenshot, logs) of the TOE generating logs for all these events.
Pass/Fail with Explanation	Pass. For each period configured, the evaluator has established a remote interactive session with the TOE and then the evaluator has observed that the session was terminated after the configured time period. This meets the testing requirements.

6.41 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	- Log into the TOE through a directly connected interface. - Verify via log that the user has logged in. - Using the instructions provided by the user guide, log out of the TOE. - Verify via log that the user has logged out.
Expected Test Results	- Evidence (Screenshot) of the evaluator locally logging into the TOE. - Evidence (Screenshot) of the evaluator terminating the local session. - Evidence (Screenshot) of the TOE generating logs for the session login and logout.
Pass/Fail with Explanation	Pass. The evaluator has initiated an interactive local session with the TOE and by following the guidance documentation has also logged out the session and observed that the session has been terminated. This meets the testing requirements.

6.42 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	- Log into the TOE Remotely. - Verify via log that the user has logged in. - Using the instructions provided by the user guide, log out of the TOE. - Verify with the log that user has logged out.
Expected Test Results	- Evidence (Screenshot) of the evaluator remotely logging into the TOE. - Evidence (Screenshot) of the evaluator terminating the remote session. - Evidence (Screenshot) of the TOE generating logs for the session login and logout.
Pass/Fail with Explanation	Pass. The evaluator has initiated an interactive remote session with the TOE and by following the guidance documentation has also logged out the session and observed that the session has been terminated. This meets the testing requirements.

6.43 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	- Configure a local time out period of 1 minute for administrative sessions.

	• Connect to the TOE from the local connection. • Verify the time. • Let the local connection set idle for 1 minute and verify that the session was terminated. • Verify that a log entry was generated for the session termination. • Configure a local time out period of 2 minutes for administrative sessions. • Connect to the TOE from the local connection. • Verify the time. • Let the local connection set idle for 2 minutes and verify that the session was terminated. • Verify that a log entry was generated for the session termination.
Expected Test Results	• Evidence showing (Screenshots) that for each period configured, the evaluator established local interactive session with the TOE and then the evaluator observed that the session was terminated after the configured time period. • Evidence (screenshot) of the TOE being configured for 1 minute of the local session idle time. • Evidence (screenshot) of the evaluator verifying the current time on the TOE. • Evidence (screenshot) of TOE's local session ending when waiting past the timeout expiration. • Evidence (screenshot, logs) of the TOE generating logs for all these events. • Evidence (screenshot) of the TOE being configured for 2 minutes of the local session idle time. • Evidence (screenshot) of the evaluator verifying the current time on the TOE. • Evidence (screenshot, logs) of the TOE generating logs for all these events.
Pass/Fail with Explanation	Pass. For each time period configured, the evaluator has established local interactive session with the TOE and then the evaluator has observed that the session was terminated after the configured time period. This meets the testing requirements.

6.44 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	• Configure an access banner for each administrative interface. • Verify that the administrative access banner is displayed for the local CLI. • Login into the TOE via the local console. • Verify that the administrative access banner is displayed for the remote CLI over SSH. • Login into the TOE via the remote CLI over SSH.

Expected Test Results	- Evidence (screenshot) showing the configured login-banner for each administrative interface of the TOE. - Evidence (screenshot) showing the banner being visible in local sessions. - Evidence (screenshot) showing the banner being visible in remote sessions over SSH.
Pass/Fail with Explanation	Pass. The evaluator has verified that the notice and consent warning message is displayed in each instance. This meets the testing requirements.

6.45 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 course of the evaluation, setting up the connections as described in the guidance documentation and ensuring that communication is successful.
Test Steps	- Initiate a remote CLI connection via SSH with the TOE. - Perform a packet capture of the traffic between the TOE and the remote administrator and verify that the data is not sent in plaintext. - Verify that the connection is connection is successful via logs.
Expected Test Results	Evidence showing (Screenshots) that the remote administration method is tested, and the connection is successful.
Pass/Fail with Explanation	Pass. It has been verified that the remote administration method is tested and the connection was successful with the data being encrypted. This meets the testing requirements.

6.46 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	- Initiate a remote CLI connection via SSH with the TOE. - Perform a packet capture of the traffic between the TOE and the remote administrator and verify that the data is not sent in plaintext. - Verify that the session was established via logs.
Expected Test Results	Evidence showing (Screenshots) that for communication channel, the channel data is not sent in plaintext

Pass/Fail with Explanation	This testing has been covered by the requirements in FTP_TRP.1/Admin Test #1 which shows that the channel data is encrypted. This meets the testing requirements.

6.47 FCS_SSHS_EXT.1.2 Test #1

Item	Data
Test Assurance Activity	Test 1: For each supported client public-key authentication algorithm, the evaluator shall configure a remote client to present a public key corresponding to that authentication method (e.g., 2048-bit RSA key when using ssh-rsa public key). The evaluator shall establish sufficient separate SSH connections with an appropriately configured remote non-TOE SSH client to demonstrate the use of all applicable public key algorithms. It is sufficient to observe the successful completion of the SSH Authentication Protocol to satisfy the intent of this test. **TD0631 has been applied.**
Test Steps	• Generate a rsa public key pair on the VM. • Copy the public key onto the TOE and verify that it is updated on the TOE. • Login to the TOE using the public key and verify that the session is established. • Verify via logs that the session was established successfully. • Verify the same via packet capture.
Expected Test Results	• Evidence (screenshots, logs, packet capture) showing that the remote client is able to establish a successful SSH connection using the supported public key algorithm.
Pass/Fail with Explanation	Pass. The remote client is able to establish a successful SSH connection using the supported public key algorithm.

6.48 FCS_SSHS_EXT.1.2 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall choose one client public key authentication algorithm supported by the TOE. The evaluator shall generate a new client key pair for that supported algorithm without configuring the TOE to recognize the associated 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. **TD0631 has been applied.**
Test Steps	• Generate a new client key pair with rsa on the VM. • Verify that the public key configured on the TOE does not match with the new public key. • Login to the device using public key without updating the public key on the TOE and verify that the connection fails.

	• Verify via audit logs that the connection fails. • Verify via packet capture that the connection fails.
Expected Test Results	• Evidence (screenshots, logs, packet capture) showing that the TOE is not able to establish a connection with a remote SSH client when the TOE is not configured to recognize the associated public key for authentication.
Pass/Fail with Explanation	Pass. The TOE is not able to establish a connection with a remote SSH client when the TOE is not configured to recognize the associated public key for authentication. This meets the testing requirements.

6.49 FCS_SSHS_EXT.1.2 Test #3

Item	Data
Test Assurance Activity	Test 3: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, 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 connecting SSH client. **TD0631 has been applied.**
Test Steps	• Configure the TOE to ensure that the TOE supports password-based authentication. • Log into the TOE via SSH with password-based authentication. • Verify via audit logs that the connection was established successfully. • Verify the same via packet capture.
Expected Test Results	• Evidence (screenshots, logs, packet capture) showing that the user authentication succeeds when the correct password is provided by the connecting SSH client.
Pass/Fail with Explanation	Pass. The TOE is able to establish a connection with a remote SSH user when correct authentication credentials are presented. This meets the testing requirements.

6.50 FCS_SSHS_EXT.1.2 Test #4

Item	Data
Test Assurance Activity	Test 4: [Conditional] If password-based authentication method has been selected in the FCS_SSHS_EXT.1.2, the evaluator shall configure the TOE to accept password-based authentication and demonstrate that user authentication fails when the incorrect password is provided by the connecting SSH client. **TD0631 has been applied.**
Test Steps	• Attempt to log into the TOE via SSH with password-based authentication and provide incorrect password (This will fail). • Verify that the authentication logs reflect failures.

	• Verify the same via packet capture.
Expected Test Results	• Evidence (screenshots, logs, packet capture) showing that the user authentication fails when incorrect password is provided by the connecting SSH client.
Pass/Fail with Explanation	Pass. The TOE is not able to establish a connection with a remote SSH user when incorrect authentication credentials are presented. This meets the testing requirements.

6.51 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	• Establish an SSH connection to the TOE using acumen-sshs tool and verify that the TOE drops the packet larger than the allowed range. • Verify with the same via packet captures.
Expected Test Results	• Evidence (screenshots, packet capture) showing that the TOE drops the packet larger than the allowed range.
Pass/Fail with Explanation	Pass. The TOE drops large packets that are received within the established SSH session. This meets the testing requirements.

6.52 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	• Configure the TOE for SSH. • Configure the TOE to support the ciphers specified in the ST. • Connect to the TOE using AES128-ctr (claimed cipher).

	• Verify that the SSH session was encrypted using AES128-ctr via logs. • Verify that the SSH session was encrypted using AES128-ctr via packet capture. • Connect to the TOE using AES256-ctr (claimed cipher). • Verify that the SSH session was encrypted using AES256-ctr via logs. • Verify that the SSH session was encrypted using AES256-ctr via packet capture. • Connect to the TOE using AES128-cbc (claimed cipher). • Verify that the SSH session was encrypted using AES128-cbc via logs. • Verify that the SSH session was encrypted using AES128-cbc via packet capture. • Connect to the TOE using AES256-cbc (claimed cipher). • Verify that the SSH session was encrypted using AES256-cbc via logs. • Verify that the SSH session was encrypted using AES256-cbc via packet capture. • Connect to the TOE using AES192-cbc (unclaimed cipher).
Expected Test Results	• Evidence (screenshots, packet captures) showing that the TOE supports all the ciphers claimed in the ST.
Pass/Fail with Explanation	Pass. It has been verified that the TOE does not support one or more additional ciphers which is not defined in the TSS for SSH.

6.53 FCS_SSHS_EXT.1.5 Test #1

Item	**Data**
Test Assurance Activity	Test 1: The evaluator shall configure (only if required by the TOE) the TOE to use each of the claimed host public key algorithms. The evaluator will then use an SSH client to confirm that the client can authenticate the TOE server public key using the claimed algorithm. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test. **TD0631 has been applied.**
Test Steps	• Connect to the TOE via SSH with SSH-RSA (supported) based host public key authentication. • Verify that the authentication takes place successfully via packet capture. • Verify the same via authentication logs.
Expected Test Results	• Evidence (screenshot, packet captures) showing that the TOE accepts connection with the claimed host public key algorithms.

Pass/Fail with Explanation	Pass. The TOE accepts connection with the claimed host public key algorithms.

6.54 FCS_SSHS_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	Test 2: The evaluator shall configure a non-TOE SSH client to only allow it to authenticate an SSH server host public key algorithm that is not included in the ST selection. The evaluator shall attempt to establish an SSH connection from the non-TOE SSH client to the TOE SSH server and observe that the connection is rejected. **TD0631 has been applied.**
Test Steps	• Connect to the TOE via SSH with RSA-SHA2-512 (not supported) based host public key authentication. • Verify authentication failure via packet capture. • Verify with logs.
Expected Test Results	• Evidence (screenshot, packet captures) showing that the TOE rejects connection with the unclaimed host public key algorithms.
Pass/Fail with Explanation	Pass. The SSH connection from the non-TOE SSH client to the TOE SSH server was rejected when unclaimed host public key algorithm was used.

6.55 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	• Configure the TOE to support the MAC algorithms specified in the ST, including, hmac-sha1, hmac-sha2-256, hmac-sha2-512. • Establish an SSH session to the TOE with hmac-sha1. • Verify that the SSH session was encrypted using the specified MAC via packet capture. • Verify through the TOE’s logs that the SSH session was successfully established. • Establish an SSH session to the TOE with hmac-sha2-256.

	• Verify that the SSH session was encrypted using the specified MAC via packet capture. • Verify through the TOE's logs that the SSH session was successfully established. • Establish an SSH session to the TOE with hmac-sha2-512. • Verify that the SSH session was encrypted using the specified MAC via packet capture. • Verify through the TOE's logs that the SSH session was successfully established.
Expected Test Results	• Evidence (screenshots, packet captures) showing that the TOE is able to establish SSH connections with each claimed data integrity algorithm
Pass/Fail with Explanation	Pass. The TOE establishes successful connection with each claimed data integrity algorithm. This meets the testing requirements.

6.56 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	• Attempt to establish an SSH session using an unsupported mac algorithm (hmac-md5). • Verify the failure in establishing a connection via packet capture. • Verify the same via logs.
Expected Test Results	• Screenshot of the TOE attempting a connection to the server using unsupported mac algorithm (hmac-md5). • Logs from the TOE showing an unsuccessful connection to the server.
Pass/Fail with Explanation	Pass. The connection is terminated due to the mismatch between the MAC algorithm proposed by the client and the MAC algorithms supported by the TOE. This meets the testing requirements.

6.57 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	• Attempt to establish an SSH session using diffie-hellman-group1-sha1. • Verify the failure in logs.

	- Verify the failure in packet capture.
Expected Test Results	- Screenshot of the server's configuration file only supporting diffie-hellman-group1-sha1. - Evidence (screenshot, packet captures) showing that the TOE does not permit connections when using diffiehellman-group1-sha1.
Pass/Fail with Explanation	Pass. The TOE doesn't establish a SSH connection with the remote client when it uses 'diffie-hellman-group1-sha1' as the Key Exchange Algorithm. This meets the testing requirements.

6.58 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	- Configure the TOE to support the claimed key exchange methods specified in the ST, including, diffie-hellman-group14- sha1, diffie-hellman-group14-sha256 and diffie-hellman-group16-sha512. - Establish an SSH session to the TOE using diffie-hellman-group14- sha1. - Verify that the SSH session was encrypted using the specified key exchange method via packet capture. - Verify through the TOE's logs that the SSH session was successfully established. - Establish an SSH session to the TOE using diffie-hellman-group14-sha256. - Verify that the SSH session was encrypted using the specified key exchange method via packet capture. - Verify through the TOE's logs that the SSH session was successfully established. - Establish an SSH session to the TOE using diffie-hellman-group16-sha512. - Verify that the SSH session was encrypted using the specified key exchange method via packet capture. - Verify through the TOE's logs that the SSH session was successfully established.
Expected Test Results	- Screenshot of the configuration on TOE using the claimed key exchange methods including diffie-hellman-group14- sha1 and diffie-hellman-group14-sha256 and diffie-hellman-group16-sha512.
Pass/Fail with Explanation	Pass. The TOE establishes successful connection with each claimed data key exchange methods. This meets the testing requirements.

6.59 FCS_SSHS_EXT.1.8 Test #1t

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	• Configure the TOE to set rekey time limit to 3 minutes. • From an SSH client, establish an SSH connection to the TOE using the verbose option for the re-key to be visible. • Keep the connection alive for a sufficient amount of time period to trigger a rekey (note that this time cannot be any more than 1 hour) and verify that a rekey was initiated after the configured time period (3 minutes) by reviewing the logs on the SSH client. • Verify via packet capture that the connection was established successfully.
Expected Test Results	• Evidence (screenshots, packet captures) showing that the TOE issues a rekey after the specified time as configured on the TOE.
Pass/Fail with Explanation	Pass. The TOE initiates a rekey frequently as per the threshold time value configured on the server.

6.60 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 WiFi radio chip is the root cause of such limitation, these chips must be identified.
Test Steps	• Configure the TOE to set rekey data limit to 10 mb. • From an SSH client, establish an SSH connection to the TOE using the verbose option for the re-key to be visible and verify that a rekey was initiated. • 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) and verify that a rekey was initiated. • Verify via packet capture that the connection was established successfully.
Expected Test Results	• Evidence (screenshots, packet captures) showing that the TOE issues a rekey after the specified amount of data transferred as configured on the TOE.
Pass/Fail with Explanation	Pass. The TOE initiated a rekey as per the data threshold configured on the TOE.

6.61 FCS_IPSEC_EXT.1.1 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The selectors used in the construction of the rule shall be different such that the evaluator can generate a packet and send packets to the gateway with the appropriate fields (fields that are used by the rule - e.g., the IP addresses, TCP/UDP ports) in the packet header. The evaluator performs both positive and negative test cases for each type of rule (e.g. a packet that matches the rule and another that does not match the rule). The evaluator observes via the audit trail, and packet captures that the TOE exhibited the expected behavior: appropriate packets were dropped, allowed to flow without modification, encrypted by the IPsec implementation.

Test Steps	**PERMIT** **POSITIVE TEST** • Configure the TOE for with an SPD covering permit. • Configure an IPsec connection to the TOE peer. • Send traffic that is protected. • Verify that each ACL was enforced via packet capture. **NEGATIVE TEST** • Send traffic that does not match the configured ACL. • Verify that the ICMP packets were allowed and SSH packets were not allowed. **DENY** **POSITIVE TEST** • Configure the TOE for with an SPD covering deny. • Configure the peer for with an SPD covering deny. • Attempt to establish the connection. • Verify the failed connection with logs. • Verify that the packets were denied via the packet capture. **NEGATIVE TEST** • Attempt to establish an SSH connection. • Verify that only the SSH packets were allowed and no ICMP packets were allowed via the packet capture. **BYPASS** **POSITIVE TEST** • Create an ACL to Bypass traffic from a host and then apply it to the respective interface.

	• Attempt to establish the connection using the networks which do not belong to the configured ACL. • Verify that the packets were bypassed via packet capture. **NEGATIVE TEST** • Send traffic that matches the configured ACL. • Verify that the packets were not bypassed via packet capture.
Expected Test Results	• The TOE should be able to implement rules for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. • Evidence (screenshot or CLI output) of configuring the SPD. • Packet capture showing each traffic flow.
Pass/Fail with Explanation	Pass. The TOE dropped packets when configured, encrypted packets when configured, and sent packets in plaintext when configured. This meets the testing requirements.

6.62 FCS_IPSEC_EXT.1.1 Test #2

Item	Data
Test Assurance Activity	The evaluator shall devise several tests that cover a variety of scenarios for packet processing. As with Test 1, the evaluator ensures both positive and negative test cases are constructed. These scenarios must exercise the range of possibilities for SPD entries and processing modes as outlined in the TSS and guidance documentation. Potential areas to cover include rules with overlapping ranges and conflicting entries, inbound and outbound packets, and packets that establish SAs as well as packets that belong to established SAs. The evaluator shall verify, via the audit trail and packet captures, for each scenario that the expected behavior is exhibited, and is consistent with both the TSS and the guidance documentation.
Test Steps	**PART-1** **Mutually Exclusive Rules** • Configure the IP filter to meet the following requirements: ○ Allow (PROTECT) a large set of traffic (e.g., TCP/IP, subnet) and Deny (DISCARD) a subset of the traffic (e.g., specific protocol, specific address). • Send the relevant traffic. • Verify that the packets belonging to a specific protocol (SSH) are denied and traffic belonging to a larger superset of traffic (TCP) are allowed. • Verify the same via logs.

PART-2

Conflicting rules

- Configure the IP filter to meet the following requirements:
    - Send a large set of traffic (e.g., TCP/UDP, subnet).
- Send relevant traffic.
- Verify that the relevant packets for the IP address mentioned in the deny rule were dropped and those for the rest of the subnet are allowed.
- Verify the same via logs.

PART-3

Overlapping rules

- Configure filter meeting the following: -
    - Allow a small set of the traffic (e.g., specific protocol, specific address).
    - Allow a larger superset of traffic (e.g., TCP/UDP, subnet).
- Send the relevant traffic.
- Verify that the traffic through both the specific protocol (SSH) as well as the larger superset of traffic (TCP) is allowed.
- Verify that the connection is not dropped.

PART-4

Packets that belong to established SAs

- Configure filter meeting the following: -
    - Packets that belong to established SAs
- Send relevant traffic.
- Verify via packet capture that the packets are dropped.
- Verify the same via logs.
- Verify that the tunnel is being established without the filter.

	- Send traffic that is protected. - Verify via packet capture that the tunnel is being established.
Expected Test Results	- The TOE should be able to permit, deny, and bypass the traffic in sequence when configured. - Evidence (screenshot or CLI output) of configuring the SPD. - Packet capture showing traffic flow.
Pass/Fail with Explanation	Pass. The TOE dropped packets when configured, encrypted packets when configured, and sent packets in plaintext when configured. This meets the testing requirements.

6.63 FCS_IPSEC_EXT.1.2 Test #1

Item	**Data**
Test Assurance Activity	evaluator shall configure the SPD such that there is a rule for dropping a packet, encrypting a packet, and allowing a packet to flow in plaintext. The evaluator may use the SPD that was created for verification of FCS_IPSEC_EXT.1.1. The evaluator shall construct a network packet that matches the rule to allow the packet to flow in plaintext and send that packet. The evaluator should observe that the network packet is passed to the proper destination interface with no modification. The evaluator shall then modify a field in the packet header; such that it no longer matches the evaluator-created entries (there may be a “TOE created” final entry that discards packets that do not match any previous entries). The evaluator sends the packet and observes that the packet was dropped.
Test Steps	- Create an access list at TOE which will allow packets to flow in plaintext. - Create an access list at peer which will allow packets to flow in plaintext. - Generate the traffic to establish the connection. - Verify the packet capture. - Verify the logs. - Modify the packet header and send the request. - Verify via packet capture.
Expected Test Results	- The TOE should be able to drop packets with modified header. - Failed connection is showed via Logs, CLI output, and packet captures.
Pass/Fail with Explanation	Pass. When the modified packet is sent, the TOE rejects the connection. This meets the testing requirements.

6.64 FCS_IPSEC_EXT.1.3 Test #1

Item	**Data**

Test Assurance Activity	If **tunnel mode** is selected, the evaluator uses the guidance documentation to configure the TOE to operate in tunnel mode and also configures a VPN peer to operate in tunnel mode. The evaluator configures the TOE and the VPN peer to use any of the allowable cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator shall then initiate a connection from the TOE to connect to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the tunnel mode.
Test Steps	• Configure the TOE for a Tunnel Mode configuration. • Create traffic that will trigger the IPsec Tunnel of the IPsec Peer. • Verify that an IKE session and tunnel was established successfully. • Verify via log that tunnel mode was used. • Verify via packet capture that tunnel mode was used.
Expected Test Results	• The TOE should be able to perform a successful connection using tunnel mode. • Evidence (screenshot or CLI output) of configuring the IPsec session. • Log showing that the IPsec session was in tunnel mode. • Packet capture showing session was in tunnel mode.
Pass/Fail with Explanation	Pass. The TOE is configured to support tunnel mode of operation. This meets the testing requirements.

6.65 FCS_IPSEC_EXT.1.3 Test #2

Item	Data
Test Assurance Activity	Test 2: If **transport mode** is selected, the evaluator uses the guidance documentation to configure the TOE to operate in transport mode and also configures a VPN peer to operate in transport mode. The evaluator configures the TOE and the VPN peer to use any of the allowed cryptographic algorithms, authentication methods, etc. to ensure an allowable SA can be negotiated. The evaluator then initiates a connection from the TOE to connect to the VPN peer. The evaluator observes (for example, in the audit trail and the captured packets) that a successful connection was established using the transport mode.
Pass/Fail with Explanation	NA. The ST does not select '**transport mode** '.

6.66 FCS_IPSEC_EXT.1.4 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the TOE as indicated in the guidance documentation configuring the TOE to use each of the supported algorithms, attempt to establish a connection using ESP, and verify that the attempt succeeds.
Test Steps	**IKEv1**

- Configure the TOE for IKEv1 AES-CBC-128 & SHA-1 configuration in ESP.
- Configure the PEER for IKEv1 AES-CBC-128 & SHA-1 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-128 & SHA-1.
- Verify via packet capture that the connection was successful using AES-CBC-128 & SHA-1.

- Configure the TOE for IKEv1 AES-CBC-192 & sha-256 configuration in ESP.
- Configure the PEER for IKEv1 AES-CBC-192 & sha-256 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-192 & SHA256 in ESP.
- Verify via packet capture that the connection was successful using AES-CBC-192 & SHA256 in ESP.

- Configure the TOE for IKEv1 AES-CBC-192 & sha-384 configuration in ESP.
- Configure the PEER for IKEv1 AES-CBC-192 & sha-384 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-256 & SHA384 in ESP.
- Verify via packet capture that the connection was successful using AES-CBC-256 & SHA384 in ESP.

- Configure the TOE for IKEv1 AES-CBC-256 & sha-512 configuration in the ESP.
- Configure the PEER for IKEv1 AES-CBC-256 & sha-512 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-256 & SHA512 in ESP.
- Verify via packet capture that the connection was successful using AES-CBC-256 & SHA512 in ESP.

- Configure the TOE for IKEv1 AES-CBC-128 & sha-256 in ESP.
- Configure the PEER for IKEv1 AES-CBC-128 & sha-256 in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established using AES-CBC-128 & sha256 in ESP.
- Verify via packet capture that the connection was established using AES-CBC-128 & sha256 in ESP.

- Configure the TOE for IKEv1 AES-CBC-192 & SHA-1 configuration in ESP.
- Configure the PEER for IKEv1 AES-CBC-192 & SHA-1 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established using AES-CBC-192 & SHA1 in ESP.

- Verify via packet capture that the connection was established using AES-CBC-192 & SHA1 in ESP.

- Configure the TOE for IKEv1 AES-CBC-256 & sha-1 configuration in the ESP.
- Configure the PEER for IKEv1 AES-CBC-256 & sha-1 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-256 & SHA1 in ESP.
- Verify via packet capture that the connection was successful using AES-CBC-256 & SHA1 in ESP.

- Configure the TOE for IKEv1 AES-CBC-128 & sha-384 configuration in ESP.
- Configure the PEER for IKEv1 AES-CBC-128 & sha-384 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-128 & SHA384 in ESP.
- Verify via packet capture that the connection was successful using AES-CBC-128 & SHA384 in ESP.

- Configure the TOE for IKEv1 AES-CBC-128 & sha-512 configuration in ESP.
- Configure the PEER for IKEv1 AES-CBC-128 & sha-512 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-128 & SHA512 in ESP.
- Verify via packet capture that the connection was successful using AES-CBC-128 & SHA512 in ESP.

- Configure the TOE for IKEv1 AES-CBC-192 & SHA-512 configuration in ESP.
- Configure the PEER for IKEv1 AES-CBC-192 & SHA-512 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established using AES-CBC-192 & SHA512 in ESP.
- Verify via packet capture that the connection was established using AES-CBC-192 & SHA512 in ESP.

- Configure the TOE for IKEv1 AES-CBC-256 & sha-256 configuration in the ESP.
- Configure the PEER for IKEv1 AES-CBC-256 & sha-256 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-256 & SHA256 in ESP.
- Verify via packet capture that the connection was successful using AES-CBC-256 & SHA256 in ESP.

- Configure the TOE for IKEv1 AES-CBC-256 & sha-384 configuration in the ESP.

- Configure the PEER for IKEv1 AES-CBC-256 & sha-384 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was successful using AES-CBC-256 & SHA384 in ESP.
- Verify via packet capture that the connection was successful using AES-CBC-256 & SHA384 in ESP.

IKEv2

- Configure the TOE for IKEv2 AES-CBC-128 & SHA-1 configuration in ESP.
- Configure the PEER for IKEv2 AES-CBC-128 & SHA-1 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established using AES-CBC-128 & SHA1.
- Verify via packet capture that the connection was established using AES-CBC-128 & SHA1.

- Configure the TOE for IKEv2 AES-CBC-192 & sha-256 configuration in ESP.
- Configure the PEER for IKEv2 AES-CBC-192 & sha-256 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established using AES-CBC-256 & sha192.
- Verify via packet capture that the connection was established using AES-CBC-256 & sha192.

- Configure the TOE for IKEv2 AES-CBC-192 & sha-384 configuration in ESP.
- Configure the PEER for IKEv2 AES-CBC-192 & sha-384 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established
- Verify via packet capture that the connection was established using AES-CBC-192 & sha384.

- Configure the TOE for IKEv2 AES-CBC-256 & sha-512 configuration in the ESP.
- Configure the PEER for IKEv2 AES-CBC-256 & sha-512 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established
- Verify via packet capture that the connection was established using AES-CBC-256 & SHA512.

- Configure the TOE for IKEv2 AES-CBC-128 & SHA-256 configuration in ESP.
- Configure the PEER for IKEv2 AES-CBC-128 & SHA-256 configuration in ESP.
- Start an IPsec connection using Ping.

- Verify via logs that the connection was established
- Verify via packet capture that the connection was established using AES-CBC-128 & SHA256.

- Configure the TOE for IKEv2 AES-CBC-128 & SHA-384 configuration in ESP.
- Configure the PEER for IKEv2 AES-CBC-128 & SHA-384 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established using AES-CBC-128 & SHA384.
- Verify via packet capture that the connection was established using AES-CBC-128 & SHA384.

- Configure the TOE for IKEv2 AES-CBC-128 & SHA-512 configuration in ESP.
- Configure the PEER for IKEv2 AES-CBC-128 & SHA-512 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established using AES-CBC-128 & SHA512.
- Verify via packet capture that the connection was established using AES-CBC-128 & SHA512.

- Configure the TOE for IKEv2 AES-CBC-192 & sha-1 configuration in ESP.
- Configure the PEER for IKEv2 AES-CBC-192 & sha-1 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established
- Verify via packet capture that the connection was established using AES-CBC-192 & sha1.

- Configure the TOE for IKEv2 AES-CBC-192 & sha-512 configuration in ESP.
- Configure the PEER for IKEv2 AES-CBC-192 & sha-512 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established
- Verify via packet capture that the connection was established using AES-CBC-192 & sha512.

- Configure the TOE for IKEv2 AES-CBC-256 & sha-256 configuration in the ESP.
- Configure the PEER for IKEv2 AES-CBC-256 & sha-256 configuration in ESP.
- Start an IPsec connection using Ping.
- Verify via logs that the connection was established using AES-CBC-256 & SHA256.
- Verify via packet capture that the connection was established using AES-CBC-256 & SHA256.

	• Configure the TOE for IKEv2 AES-CBC-256 & sha-1 configuration in the ESP. • Configure the PEER for IKEv2 AES-CBC-256 & sha-1 configuration in ESP. • Start an IPsec connection using Ping. • Verify via logs that the connection was established using AES-CBC-256 & SHA1. • Verify via packet capture that the connection was established using AES-CBC-256 & SHA1. • Configure the TOE for IKEv2 AES-CBC-256 & sha-384 configuration in the ESP. • Configure the PEER for IKEv2 AES-CBC-256 & sha-384 configuration in ESP. • Start an IPsec connection using Ping. • Verify via logs that the connection was established using AES-CBC-256 & SHA384. • Verify via packet capture that the connection was established using AES-CBC-256 & SHA384.
Expected Test Results	• IPsec SAs should be configured with each claimed encryption and hash algorithm. • Evidence (screenshot or CLI output) of configuring the IPsec session. • Log showing that the IPsec session was in claimed encryption and hash algorithm. • Packet capture showing session was in claimed encryption and hash algorithm.
Pass/Fail with Explanation	Pass. This test shows that the IKE SAs can be configured with each claimed algorithm. This meets the testing requirements.

6.67 FCS_IPSEC_EXT.1.5 Test #1

Item	**Data**
Test Assurance Activity	If **IKEv1** is selected, the evaluator shall configure the TOE as indicated in the guidance documentation and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported.
Test Steps	• Configure the TOE to support IKEv1 using main mode only. • Configure peer for aggressive mode. • Attempt to establish the IPsec tunnel. • Attempt to send traffic through the IPsec tunnel. • Verify that Aggressive mode connections are not possible via packet capture. • Verify that Aggressive mode connections are not possible via log. • Configure the TOE to support IKEv1 using main mode only. • Configure the peer to support IKEv1 using main mode only. • Establish the IPsec tunnel.

	• Send traffic through the IPsec tunnel. • Verify that main mode is established in the IPsec connection via log. • Verify that main mode is established in the IPsec connection via packet capture.
Expected Test Results	• The TOE should reject a connection attempt with aggressive mode and then accept a connection attempt with main mode. • Evidence (screenshot or CLI output) of IKE configuration. • Log showing the unsuccessful and successful session attempt. • Packet capture of the unsuccessful and successful session attempt.
Pass/Fail with Explanation	Pass. The TOE rejected a connection attempt with Aggressive mode and then accepted a connection attempt with main mode. This meets the testing requirements.

6.68 FCS_IPSEC_EXT.1.5 Test #2

Item	Data
Test Assurance Activity	If **NAT traversal** is selected within the IKEv2 selection, the evaluator shall configure the TOE so that it will perform NAT traversal processing as described in the TSS and RFC 5996, section 2.23. The evaluator shall initiate an IPsec connection and determine that the NAT is successfully traversed.
Test Steps	• Configure the TOE for NAT Traversal. • Verify that the TOE is configured for NAT-T. • Configure the peer. • Establish the IPsec tunnel. • Verify NAT traversal occurred via packet capture.
Expected Test Results	• The TOE should perform a successful connection with NAT Traversal. • Evidence (screenshot or CLI output) of the configuration. • Packet capture of the successful session attempt.
Pass/Fail with Explanation	Pass. NAT is successfully traversed.

6.69 FCS_IPSEC_EXT.1.6 Test #1

Item	Data
Test Assurance Activity	The evaluator shall configure the TOE to use the ciphersuite under test to encrypt the IKEv1 and/or IKEv2 payload and establish a connection with a peer device, which is configured to only accept the payload encrypted using the indicated ciphersuite. The evaluator will confirm the algorithm was that used in the negotiation.
Test Steps	**IKEv1**

- Configure the TOE for IKEv1 using AES-CBC-128.
- Configure the Peer with an IKE1 policy using AES-CBC-128.
- Start an IPsec connection (using Ping).
- Verify via logs that the connection was established.
- Verify via packet capture that the connection was established using AES-CBC-128.

- Configure the TOE for IKEv1 using AES-CBC-192.
- Configure the Peer with an IKE1 policy using AES-CBC-192.
- Start an IPsec connection (using Ping).
- Verify via logs that the connection was established.
- Verify via packet capture that the connection was established using AES-CBC-192.

- Configure the TOE for IKEv1 using AES-CBC-256.
- Configure the Peer with an IKE1 policy using AES-CBC-256.
- Start an IPsec connection (using Ping).
- Verify via logs that the connection was established.
- Verify via packet capture that the connection was established using AES-CBC-256.

IKEv2

- Configure the TOE for IKEv2 using AES-CBC-128.
- Configure the Peer for IKEv2 using AES-CBC-128
- Start an IPsec connection (using Ping).
- Verify via logs that the connection was established.
- Verify via packet capture that the connection was established using AES-CBC-128.

- Configure the TOE for IKEv2 using AES-CBC-192.
- Configure the Peer for IKEv2 using AES-CBC-192.
- Start an IPsec connection (using Ping).
- Verify via logs that the connection was established.
- Verify via packet capture that the connection was established using AES-CBC-192.

- Configure the TOE for IKEv2 using AES-CBC-256.
- Configure the Peer for IKEv2 using AES-CBC-256.
- Start an IPsec connection (using Ping).
- Verify via logs that the connection was established using AES-CBC-256.

	• Verify via packet capture that the connection was established using AES-CBC-256.
Expected Test Results	• IKE should be configured with each claimed cipher suite. • Evidence (screenshot or CLI output) of configuring the IKE session. • Log showing that the IKE session was in claimed cipher suite. • Packet capture showing IKE session was in claimed cipher suite.
Pass/Fail with Explanation	Pass. IKE SAs can be configured with each claimed algorithm. This meets the testing requirements.

6.70 FCS_IPSEC_EXT.1.7 Test #1

Item	Data
Test Assurance Activity	Test 1: If '**number of bytes**' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime in terms of the number of bytes allowed following the guidance documentation. The evaluator shall configure a test peer with a byte lifetime that exceeds the lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer, and determine that once the allowed number of bytes through this SA is exceeded, a new SA is negotiated. The evaluator shall verify that the TOE initiates a Phase 1 negotiation.
Pass/Fail with Explanation	NA. The ST does not select '**number of bytes**'.

6.71 FCS_IPSEC_EXT.1.7 Test #2

Item	Data
Test Assurance Activity	Test 2: If '**length of time**' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime of 24 hours for the Phase 1 SA following the guidance documentation. The evaluator shall configure a test peer with a lifetime that exceeds the lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer, maintain the Phase 1 SA for 24 hours, and determine that a new Phase 1 SA is negotiated on or before 24 hours has elapsed. The evaluator shall verify that the TOE initiates a Phase 1 negotiation. **TD0633 has been applied.**
Test Steps	**IKEv1** • Configure the Phase 1 lifetime (isakmp-lifetime) on the TOE to less than 24 hours (82800 seconds). • Configure the Phase 1 lifetime (ike lifetime) on the Strongswan Peer to 24 hours (86400 seconds). • Configure the "auto-establish" part in the IPsec tunnel configuration so that the TOE initiates the re-key.

	• Start a connection through the Peer and maintain the connection. • Verify the rekey occurred via Packet Capture. **IKEv2** • Configure the Phase 1 lifetime (isakmp-lifetime) on the TOE to less than 24 hours (82800 seconds). • Configure the Phase 1 lifetime (ike lifetime) on the Strongswan Peer to 24 hours (86400 seconds). • Configure the "auto-establish" part in the IPsec tunnel configuration so that the TOE initiates the re-key. • Start a connection through the Peer and maintain the connection. • Verify the rekey occurred via Packet Capture.
Expected Test Results	• The TOE should renegotiate phase 1 after the lifetime exceeds the configured phase 1 lifetime of the TOE. • Evidence (screenshot) showing configuration of IKE lifetime. • Packet capture showing the phase 1 lifetime threshold is met.
Pass/Fail with Explanation	Pass. The TOE renegotiates phase 1 after the lifetime exceeds the lifetime of the TOE. This meets the testing requirements.

6.72 FCS_IPSEC_EXT.1.8 Test #1

Item	Data
Test Assurance Activity	Test 1: If '**number of bytes**' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime in terms of the number of bytes allowed following the guidance documentation. The evaluator shall configure a test peer with a byte lifetime that exceeds the lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer, and determine that once the allowed number of bytes through this SA is exceeded, a new SA is negotiated. The evaluator shall verify that the TOE initiates a Phase 2 negotiation.
Pass/Fail with Explanation	NA. The ST does not select '**number of bytes**'.

6.73 FCS_IPSEC_EXT.1.8 Test #2

Item	Data
Test Assurance Activity	Test 2: If '**length of time**' is selected as the SA lifetime measure, the evaluator shall configure a maximum lifetime of 8 hours for the Phase 2 SA following the guidance documentation. The evaluator shall configure a test peer with a lifetime that exceeds the lifetime of the TOE. The evaluator shall establish a SA between the TOE and the test peer, maintain the Phase 1 SA for 8 hours, and determine

	that once a new Phase 2 SA is negotiated when or before 8 hours has lapsed. The evaluator shall verify that the TOE initiates a Phase 2 negotiation. **TD0633 has been applied.**
Test Steps	**IKEv1** • Configure the Phase 2 IPsec lifetime as 7 hours (25200 seconds) on the TOE. • Configure the “auto-establish” part in the IPsec tunnel configuration so that the TOE initiates the re-key. • Configure the Phase 2 IPsec lifetime of the Strongswan peer to be greater than the Phase 2 lifetime configured on the TOE (28800 seconds). • Start a connection through the Peer and maintain the connection. • Verify the rekey occurred via Packet Capture. **IKEv2** • Configure the Phase 2 IPsec lifetime as 7 hours (25200 seconds) on the TOE. • Configure the “auto-establish” part in the IPsec tunnel configuration so that the TOE initiates the re-key. • Configure the Phase 2 IPsec lifetime of the Strongswan peer to be greater than the Phase 2 lifetime configured on the TOE (28800 seconds). • Start a connection through the Peer and maintain the connection. • Verify the rekey occurred via Packet Capture.
Expected Test Results	• The TOE should renegotiate phase 2 after the lifetime exceeds the configured phase 2 lifetime of the TOE. • Evidence (screenshot) showing configuration of IKE lifetime. • Packet capture showing the phase 1 lifetime threshold is met.
Pass/Fail with Explanation	Pass. This test case shows that when configured for rekey the TOE will rekey at the configured time interval. This meets the testing requirements.

6.74 FCS_IPSEC_EXT.1.10 Test #1

Item	Data
Test Assurance Activity	Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection: If the first selection is chosen, the evaluator shall check to ensure that, for each DH group supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.

Test Output	**Covered by TSS Assurance Activities in the AAR.**
Pass/Fail with Explanation	Pass. This test has been covered by the requirements in **TSS Assurance Activities in the AAR.**

6.75 FCS_IPSEC_EXT.1.10 Test #2

Item	**Data**
Test Assurance Activity	Each of the following tests shall be performed for each version of IKE selected in the FCS_IPSEC_EXT.1.5 protocol selection: If the second selection is chosen, the evaluator shall check to ensure that, for each PRF hash supported, the TSS describes the process for generating each nonce. The evaluator shall verify that the TSS indicates that the random number generated that meets the requirements in this PP is used, and that the length of the nonces meet the stipulations in the requirement.
Test Output	**Covered by TSS Assurance Activities in the AAR.**
Pass/Fail with Explanation	Pass. This test has been covered by the requirements in **TSS Assurance Activities in the AAR.**

6.76 FCS_IPSEC_EXT.1.11 Test #1

Item	**Data**
Test Assurance Activity	For each supported DH group, the evaluator shall test to ensure that all supported IKE protocols can be successfully completed using that particular DH group.
Test Steps	**IKEv1** • Configure DH group 14 for IKEv1 on TOE. • Configure DH group 14 for IKEv1 on the Peer. • Start an IPsec connection. • Verify that Group 14 is used via capture. • Configure DH group 15 for IKEv1 on TOE. • Configure DH group 15 for IKEv1 on the Peer. • Start an IPsec connection. • Verify that Group 15 is used via capture. **IKEv2** • Configure DH group 14 for IKEv2 on TOE.

	- Configure DH group 14 for IKEv2 on the Peer. - Start an IPsec connection. - Verify that Group 14 is used via capture. - Configure DH group 15 for IKEv2 on TOE. - Configure DH group 15 for IKEv1 on the Peer. - Start an IPsec connection. - Verify that Group 15 is used via capture.
Expected Test Results	- IKE SAs should be configured with each claimed exchange method. - Evidence (screenshot) showing the IKE policy configuration. - Packet capture showing that only particular DH group was used.
Pass/Fail with Explanation	Pass. This test showed that the DH Group used in IPsec connections is configurable. This meets the testing requirements.

6.77 FCS_IPSEC_EXT.1.12 Test #1

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall successfully negotiate an IPsec connection using each of the supported algorithms and hash functions identified in the requirements.
Pass/Fail with Explanation	Pass. This testing will be covered by the requirements in FCS_IPSEC_EXT.1.4 Test#1 and FCS_IPSEC_EXT.1.6 Test#1.

6.78 FCS_IPSEC_EXT.1.12 Test #2

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish a SA for ESP that selects an encryption algorithm with more strength than that being used for the IKE SA (i.e., symmetric algorithm with a key size larger than that being used for the IKE SA). Such attempts should fail.
Test Steps	**IKEv1** - Configure the TOE to use AES-CBC-128 as the Phase 1 Encryption Algorithm. - Configure the TOE to use AES-CBC-256 as the Phase 2 Encryption Algorithm which is stronger than the Phase 1 algorithm. - Attempt to enable the IPsec tunnel and verify that this attempt fails.

	• Attempt to establish a connection. • Attempt to send traffic through the tunnel. • Verify the connection is rejected using Packet Capture. **IKEv2** • Configure the TOE to use AES-CBC-128 as the Phase 1 Encryption Algorithm. • Configure the TOE to use AES-CBC-256 as the Phase 2 Encryption Algorithm which is stronger than the Phase 1 algorithm. • Attempt to enable the IPsec tunnel and verify that this attempt fails. • Attempt to establish a connection. • Attempt to send traffic through the tunnel. • Verify the connection is rejected using Packet Capture.
Expected Test Results	• When attempting to connect to a peer with the IPsec SA strength larger than the IKE SA strength, the TOE should be able to reject the connection. • Packet capture showing the failed connection.
Pass/Fail with Explanation	Pass. The TOE rejects the IPsec connection when the ESP encryption algorithm (Phase 2) is stronger than the IKE algorithm (Phase 1). This meets the testing requirements.

6.79 FCS_IPSEC_EXT.1.12 Test #3

Item	**Data**
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish an IKE SA using an algorithm that is not one of the supported algorithms and hash functions identified in the requirements. Such an attempt should fail.
Test Steps	**IKEv1** • Configure the TOE to use AES and SHA1. • Configure the Peer to use 3DES and SHA1. • Attempt to establish an IPsec connection. • Verify the connection is rejected via packet capture. • Verify the same via logs reflected on the TOE. **IKEv2** • Configure the TOE to use AES and SHA1. • Configure the Peer to use 3DES and SHA1. • Attempt to establish an IPsec connection. • Verify the connection is rejected via packet capture.

	• Verify the same via logs reflected on the TOE.
Expected Test Results	• The TOE should only support and propose the configured algorithm. If the TOE peer does not have matching algorithms, the IPsec session should not be established. • Logs showing the failed connection. • Packet capture showing the failed connection.
Pass/Fail with Explanation	Pass. The TOE will only support and propose the configured algorithm. If the TOE and peer does not have matching algorithms this session will not be established. This meets the testing requirements.

6.80 FCS_IPSEC_EXT.1.12 Test #4

Item	Data
Test Assurance Activity	This test shall be performed for each version of IKE supported. The evaluator shall attempt to establish a SA for ESP (assumes the proper parameters where used to establish the IKE SA) that selects an encryption algorithm that is not identified in FCS_IPSEC_EXT.1.4. Such an attempt should fail.
Test Steps	**IKEv1** • Configure TOE to support AES-CBC-128 in transform set. • Configure Peer to support 3Des in Transform set. • Attempt to establish an IPsec connection between TOE and Peer. • Verify via logs that the connection is rejected. • Verify the connection is rejected using Packet Capture. **IKEv2** • Configure TOE to support AES-CBC-128 in transform set. • Configure Peer to support 3Des in Transform set. • Attempt to establish an IPsec connection between TOE and Peer. • Verify via logs that the connection is rejected. • Verify the connection is rejected using Packet Capture.
Expected Test Results	• Since the IPsec SA parameters does not match the IPsec SA parameters of the TOE peer, an IPsec connection should not be established. An IKE SA, however, should be established because the peer parameters match. • Log showing the failed connection. • Packet capture showing the failed connection.

Pass/Fail with Explanation	Pass. Since the IPsec SA parameters did not match the IPsec SA parameters of the TOE peer, an IPsec connection could not be established. An IKE SA, however, could be established because the peer parameters matched. This meets the testing requirements.

6.81 FCS_IPSEC_EXT.1.14 Test #1

Item	Data
Test Assurance Activity	Test 1: [conditional] For each CN/identifier type combination selected, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE authentication succeeds. If the TOE prioritizes CN checking over SAN (through explicit configuration of the field when specifying the reference identifier or prioritization rules), the evaluator shall also configure the SAN so it contains an incorrect identifier of the correct type (e.g. the reference identifier on the TOE is example.com, the CN=example.com, and the SAN:FQDN=otherdomain.com) and verify that IKE authentication succeeds.
Pass/Fail with Explanation	NA. The ST does not select **'CN/identifier type combination'**.

6.82 FCS_IPSEC_EXT.1.14 Test #2

Item	Data
Test Assurance Activity	Test 2: [conditional] For each SAN/identifier type combination selected, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the field in the peer's presented certificate and shall verify that the IKE authentication succeeds. If the TOE prioritizes SAN checking over CN (through explicit specification of the field when specifying the reference identifier or prioritization rules), the evaluator shall also configure the CN so it contains an incorrect identifier formatted to be the same type (e.g. the reference identifier on the TOE is DNS-ID; identify certificate has an identifier in SAN with correct DNS-ID, CN with incorrect DNS-ID (and not a different type of identifier)) and verify that IKE authentication succeeds.
Test Steps	**PART-1** • Create and load a peer certificate with a SAN IP that matches the TOE's reference identifier. • Configure the Strongswan peer's SAN IP on the TOE. • Configure the Strongswan peer. • Attempt to establish the IPsec tunnel. • Send traffic through the IPsec tunnel. • Verify that the connection is successful via packet capture. **PART-2**

	• Create and load a peer certificate with a FQDN in the SAN that matches the TOE’s reference identifier. • Import the new end-entity certificate on the TOE. • Configure the Strongswan peer’s SAN FQDN on the TOE. • Configure the Strongswan peer. • Attempt to establish the IPsec tunnel. • Send traffic through the IPsec tunnel. • Verify through packet capture that the connection succeeds. **PART-3** • Create and load a peer certificate with a User FQDN in the SAN that matches the TOE’s reference identifier. • Import the new end-entity certificate on the TOE. • Configure the Strongswan peer’s SAN User FQDN on the TOE. • Configure the Strongswan peer. • Attempt to establish the IPsec tunnel. • Send traffic through the IPsec tunnel. • Verify through packet capture that the connection succeeds.
Expected Test Results	• The TOE should accept the connection when the SAN matches with the PEER. • Logs verifying successful connection. • Packet capture verifying successful connection.
Pass/Fail with Explanation	Pass. The TOE accepts connections when the SAN matches with the PEER. This meets the testing requirements.

6.83 FCS_IPSEC_EXT.1.14 Test #3

Item	Data
Test Assurance Activity	Test 3: [conditional] For each CN/identifier type combination selected, the evaluator shall: a) Create a valid certificate with the CN so it contains the valid identifier followed by ‘\0’. If the TOE prioritizes CN checking over SAN (through explicit specification of the field when specifying the reference identifier or prioritization rules) for the same identifier type, the evaluator shall configure the SAN so it matches the reference identifier. b) Configure the peer’s reference identifier on the TOE (per the administrative guidance) to match the CN without the ‘\0’ and verify that IKE authentication fails.

Pass/Fail with Explanation	NA. The ST does not select **'CN/identifier type combination'**.

6.84 FCS_IPSEC_EXT.1.14 Test #4

Item	Data
Test Assurance Activity	Test 4: [conditional] For each SAN/identifier type combination selected, the evaluator shall: a) Create a valid certificate with an incorrect identifier in the SAN. The evaluator shall configure a string representation of the correct identifier in the DN. If the TOE prioritizes CN checking over SAN (through explicit specification of the field when specifying the reference identifier or prioritization rules) for the same identifier type, the addition/modification shall be to any non-CN field of the DN. Otherwise, the addition/modification shall be to the CN. b) Configure the peer's reference identifier on the TOE (per the administrative guidance) to match the correct identifier (expected in the SAN) and verify that IKE authentication fails.
Test Steps	**PART-1** • Create and load a peer certificate with an incorrect SAN IP but a correct IP in the CN field. • Configure the correct Strongswan peer's SAN IP on the TOE. • Configure the Strongswan peer. • Attempt to establish the IPsec tunnel. • Attempt to send traffic through the IPsec tunnel. • Verify through logs that the connection fails. • Verify via packet capture that the connection does not get established. **PART-2** • Create and load a peer certificate with an incorrect FQDN in the SAN but a correct FQDN in the CN field. • Configure the correct FQDN on the TOE's peer reference identifier. • Configure the Strongswan peer. • Attempt to establish the IPsec tunnel. • Attempt to send traffic through the IPsec tunnel. • Verify through logs that the connection fails. • Verify via packet capture that the connection does not get established.

	PART-3 • Create and load a peer certificate with an incorrect User FQDN in the SAN but a correct User FQDN in the CN field. • Configure the correct User FQDN on the TOE's peer reference identifier. • Attempt to establish the IPsec tunnel. • Attempt to send traffic through the IPsec tunnel. • Verify through logs that the connection fails. • Verify via packet capture that the connection does not get established.
Expected Results	• TOE does not establish connection with local certificate having incorrect SAN and correct CN. • TOE logs verify unsuccessful connection due to local certificate authentication failure. • Packet Capture verifies unsuccessful connection due to local certificate authentication failure.
Pass/Fail with Explanation	Pass. The TOE rejects connection when the SAN mismatches with the PEER. This meets the testing requirements.

6.85 FCS_IPSEC_EXT.1.14 Test #5

Item	Data
Test Assurance Activity	Test 5: (conditional) If the TOE supports DN identifier types, the evaluator shall configure the peer's reference identifier on the TOE (per the administrative guidance) to match the subject DN in the peer's presented certificate and shall verify that the IKE authentication succeeds
Pass/Fail with Explanation	NA. The ST does not select "**DN** identifier types".

6.86 FCS_IPSEC_EXT.1.14 Test #6a

Item	Data
Test Assurance Activity	Test 6: [conditional] If the TOE supports **DN** identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE: a) Duplicate the CN field, so the otherwise authorized DN contains two identical CNs.

Pass/Fail with Explanation	NA. The ST does not select "**DN** identifier types".

6.87 FCS_IPSEC_EXT.1.14 Test #6b

Item	Data
Test Assurance Activity	Test 6: If the TOE supports **DN** identifier types, to demonstrate a bit-wise comparison of the DN, the evaluator shall create the following valid certificates and verify that the IKE authentication fails when each certificate is presented to the TOE: b) Append '\0' to a non-CN field of an otherwise authorized DN.
Pass/Fail with Explanation	NA. The ST does not select "**DN** identifier types".

6.88 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	• Reset or reboot the TOE and ensure that the TOE performs all the claimed self-tests successfully.
Expected Test Results	• The TOE should execute all claimed self-tests during bootup. • Evidence (screenshots) of self-tests showing execution of self-tests and successful connection.
Pass/Fail with Explanation	Pass. The TOE successfully executes self-test. This meets the testing requirement.

6.89 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	• Verify the current version on the TOE. • Perform the image update. • Reload the TOE. • Verify the new version of the TOE.
Expected Test Results	Evidence (Screenshots) showing that the TOE successfully updates the current image version with the new image.
Pass/Fail with Explanation	Pass. The evaluator obtained a legitimate update using procedures described in the guidance documentation and verified that it is successfully installed on the TOE.

6.90 FPT_TUD_EXT.1 Test #2 (a)

Item	Data
Test Assurance Activity	Test 2 [conditional]: If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are 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 illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 1) A modified version (e.g. using a hex editor) of a legitimately signed update If the TOE allows a 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 an attempted update is rejected. 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.
Pass/Fail with Explanation	NA. The ST does not select "If the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE the following test shall be performed".

6.91 FPT_TUD_EXT.1 Test #2 (b)

Item	Data
Test Assurance Activity	[conditional]: If **the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE** the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are 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 illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 2) An image that has not been signed If the TOE allows a 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 an attempted update is rejected. 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.
Pass/Fail with Explanation	NA. The ST does not select "the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE".

6.92 FPT_TUD_EXT.1 Test #2 (c)

Item	Data
Test Assurance Activity	[conditional]: If **the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE** the following test shall be performed (otherwise the test shall be omitted). The evaluator first confirms that no updates are 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 illegitimate updates as defined below, and attempts to install them on the TOE. The evaluator verifies that the TOE rejects all of the illegitimate updates. The evaluator performs this test using all of the following forms of illegitimate updates: 3) An image signed with an invalid signature (e.g. by using a different key as expected for creating the signature or by manual modification of a legitimate signature) If the TOE allows a 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 an attempted update is rejected. 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.
Pass/Fail with Explanation	NA. The ST does not select “the TOE itself verifies a digital signature to authorize the installation of an image to update the TOE”.

6.93 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	• Display the hash file on the TOE. • Edit the hash file. • Reboot and verify that the console output shows that TOE failed to load the image.
Expected Test Results	• Evidence (screenshots) showing the failure of the software update when the hash file is edited.
Pass/Fail with Explanation	Pass. The evaluator has verified that TOE rejected an update when the publish hash didn't match to the hash of image.

6.94 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	• Remove the hash file from the TOE. • Verify that the hash file "hmac-sha256.txt" has been removed. • Reboot the TOE, observe the console output and verify that TOE rejected to load the image.
Expected Test Results	• Evidence (screenshots) showing the failure of the software update when the hash file is removed.
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.

6.95 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	• Upload full certificate chain to the TOE's trust store. • Verify that a log was generated when uploading the certificate chain. • Display the imported certificates. • Verify that the ca-profiles have the correct certificates and crl-files. • Configure the Strongswan peer. • Attempt to establish the IPsec tunnel between the TOE and peer. • Send traffic through the IPsec tunnel. • Verify the connection is established via packet capture.
Expected Test Results	• Once the TOE receives a valid certificate chain the IPsec tunnel gets established successfully. • Evidence (screenshots, logs, packet captures) showing successful IPsec tunnel connection.
Pass/Fail with Explanation	Pass. The TOE is able to successfully establish the connection with uploaded certificates.

6.96 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	• For TOE configurations, refer FIA_X509_EXT.1.1 Test #1a. • Remove one of the certificates from the uploaded certificate chain. • Attempt to establish connection using the IPsec tunnel without the ICA certificate. • Verify that the connection failed via packet capture. • Verify that the connection failed via logs.
Expected Test Results	• When certificate chain is broken, TOE fails to establish the connection. • Evidence (screenshots, logs, packet captures) showing unsuccessful connection.
Pass/Fail with Explanation	Pass. The evaluator has verified that an attempt to validate this broken chain failed and the TOE rejected the connection.

6.97 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	• For TOE configurations, refer FIA_X509_EXT.1.1 Test #1. • Display the chain of certificates. • Display the time on the TOE. • Verify that the connection gets established successfully using valid chain of certificates. • Send traffic through the IPsec tunnel. • Verify that the connection gets established successfully via packet capture. • Change the TOE’s system date to a date that is over the ‘NotAfter’ date on the Intermediate CA. • Attempt to establish the IPsec tunnel and verify that it fails. • Verify via logs that the connection fails due to the expired Intermediate certificate. • Verify via packet capture that the connection is rejected.
Expected Test Results	Evidence (screenshots, logs, packet captures) showing that when the TOE receives expired server certificate it fails to establish the IPsec tunnel.

Pass/Fail with Explanation	Pass. The evaluator has verified that when an expired certificate was represented, the verification got failed and TOE rejected the connection.

6.98 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	**CRL** **PART-1** • Create a valid certificate chain and upload them to the TOE and peer device. • Import the Root CA CRL and ICA CRL on the TOE. • Configure the remote CRL on the TOE. • Host the CRL files on the test VM Apache web server. • Attempt a connection between the TOE and the peer and verify that the connection is successful. **PART-2** • Revoke an intermediate certificate in the uploaded certificate chain. • Update the CRL on the TOE. • Display the CA CRL certificate. • Verify unsuccessful connection negotiation when intermediate CA certificate is revoked. • Send traffic and verify that it does not go through the tunnel. • Verify the same via logs.

	- Verify the same via packet capture. **PART 3** - Revoke end entity (peer) certificate in the uploaded certificate chain. - Update the CRL on the TOE. - Display the updated CRLs on the TOE. - Attempt a connection between the TOE and the peer and verify that the connection fails. - Send traffic and verify that it does not go through the tunnel. - TOE logs verify unsuccessful connection negotiation when end entity certificate is revoked.
Expected Test Results	- Evidence (screenshots, logs, packet captures) showing that the TOE is able to establish a successful IPsec connection with unrevoked server certificate. - Evidence (screenshots, logs, packet captures) that the IPsec connection fails when the TOE receives a revoked intermediate certificate. - Evidence (screenshots, logs, packet captures) that the IPsec connection fails when the TOE receives a revoked end entity certificate.
Pass/Fail with Explanation	Pass. The TOE successfully connects to the server with a valid certificate and does not connect to the server with a revoked certificate.

6.99 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 CRL sign key usage bit set and verify that validation of the CRL fails.
Test Steps	- Create the intermediate CA with CRL sign bit OFF. - Make sure that CA certificates are uploaded onto the TOE. - Display the valid chain of certificates and verify that the ICA certificate does not have the CRL Sign parameter. - Update the ca-profile. - Verify via logs that the TOE gives an error while updating the ca-profile. - Host the CRLs on the Apache server. - Update the CRL on the TOE. - Attempt to establish the IPsec connection.

	- Send traffic to go through the tunnel. - Verify via packet capture that the connection fails. - Verify the failure logs.
Expected Test Results	- The TOE rejects the IPsec connection when CA signing the CRL does not have the cRLsign key usage bit set. - Evidence (screenshots, logs, packet captures) showing unsuccessful connection.
Pass/Fail with Explanation	Pass. The evaluator has configured 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.

6.100 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	- Run the StrongSwan Acumen tool, using it to modify the first byte of the encoding certificate, incrementing 30 to 31. - Send traffic through the IPsec tunnel. - Verify the connection is refused via packet capture. - Verify the connection is refused via logs**.**
Expected Test Results	- The TOE rejects the IPsec connection when the first byte of the certificate is modified. - Evidence (screenshot) showing modification of certificate. - Evidence (screenshot, logs, packet capture) showing unsuccessful connection.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the first byte of the certificate is modified. This meets the testing requirements.

6.101 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	• Run the StrongSwan Acumen tool to modify the last byte of the encoding certificate by incrementing 85 to 86 and 78 to 79. • Send traffic through the IPsec tunnel. • Verify the connection is refused via packet capture. • Verify the connection is refused via logs.
Expected Test Results	• The TOE rejects the connection when the byte in the certificate SignatureValue field is modified. • Evidence (screenshot) showing modification of certificate. • Evidence (screenshot, logs, packet capture) showing unsuccessful connection.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the last byte of the certificate is modified. This meets the testing requirements.

6.102 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	• Run the StrongSwan Acumen tool to modify any byte in public key of certificate by incrementing 82 to 83. • Send traffic through the IPsec tunnel. • Verify the connection is refused via packet capture. • Verify the connection is refused via logs.
Expected Test Results	• The TOE rejects the connection when the public key of the certificate is modified. • Evidence (screenshot) showing modification of certificate. • Evidence (screenshot, logs, packet capture) showing unsuccessful connection.
Pass/Fail with Explanation	Pass. The TOE rejects connections when the public key of the certificate is modified. This meets the testing requirements.

6.103 FIA_X509_EXT.1.1/Rev Test #8a

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)**

	(Conditional on TOE ability to process CA certificates presented in certificate message) The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC 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 EC root CA certificate in the trust store). The evaluator shall present the TOE with a valid chain of EC certificates (terminating in a trusted CA certificate), where the elliptic curve parameters are specified as a named curve. The evaluator shall confirm that the TOE validates the certificate chain. **TD0527 (12/1 Update) has been applied.**
Pass/Fail with Explanation	NA. The TOE does not support EC certificates.

6.104 FIA_X509_EXT.1.1/Rev Test #8b

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** **(Conditional on TOE ability to process CA certificates presented in certificate message)** The test shall be designed in a way such that only the EC root certificate is designated as a trust anchor, and by setting up the trust store in a way that the EC 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 EC root CA certificate in the trust store). The evaluator shall present the TOE with a chain of EC certificates (terminating in a trusted CA certificate), where the intermediate certificate in the certificate chain uses an explicit format version of the Elliptic Curve parameters in the public key information field, and is signed by the trusted EC root CA, but having no other changes. The evaluator shall confirm the TOE treats the certificate as invalid. **TD0527 (12/1 Update) has been applied.**
Pass/Fail with Explanation	NA. The TOE does not support EC certificates.

6.105 FIA_X509_EXT.1.1/Rev Test #8c

Item	Data
Test Assurance Activity	**(Conditional on support for EC certificates as indicated in FCS_COP.1/SigGen)** **(Conditional on support for a minimum certificate path length of three certificates)** The evaluator shall establish a subordinate CA certificate, where the elliptic curve parameters are specified as a named curve, that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is accepted into the TOE's trust store. The evaluator shall then establish a subordinate CA certificate that uses an explicit format version of the elliptic curve parameters, and that is signed by a trusted EC root CA. The evaluator shall attempt to load the certificate into the trust store and observe that it is rejected, and not added to the TOE's trust store. **TD0527 (12/1 Update) has been applied.**

Pass/Fail with Explanation	NA. The TOE does not support EC certificates.

6.106 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 trivially 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	• Display the valid chain of certificates. • Establish the IPsec connection using the valid chain of certificates. • Send traffic through the IPsec tunnel. • Verify via packet capture that the tunnel was established successfully. • Create a certificate chain where an intermediate CA does not have the basicConstraints extension using Python script. • Verify that the original ICA certificate and the modified ICA certificate has the same serial number. • Attempt to upload the modified intermediate CA certificate to the TOE. • Attempt to add an intermediate CA certificate without basicConstraints extension to the TOE's ca-profile. • Verify that the TOE rejects the certificate chain via log. • Attempt to establish the IPsec tunnel.

	• Send traffic through the IPsec tunnel. • Verify via logs that the TOE rejects the connection. • Verify the same via packet capture.
Expected Test Results	• The TOE should reject certificates signed by CA that does not contain the basicConstraints Extension. • Evidence (screenshot) showing extensions of the ICA certificate which does not have the basicConstraints extension. • Evidence (screenshots, logs, packet capture) showing unsuccessful IPsec connection.
Pass/Fail with Explanation	Pass. The evaluator has verified that TOE rejected the IPsec connection with the ICA certificate which does not have the basicConstraints extension.

6.107 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 trivially 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: 1. As part of the validation of the leaf certificate belonging to this chain; 2. 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	• Display the valid chain of certificates. • Verify that the connection is established using valid chain of certificates. • Send traffic through the IPsec tunnel. • Verify via packet capture that the connection is getting established successfully.

	- Create a certificate chain where an intermediate CA has the basicConstraints extension configured to FALSE. - Verify that the original ICA certificate and the modified ICA certificate has the same serial number. - Verify that the CA flag in the basicConstraints extension is configured to FALSE. - Attempt to upload the certificate to the TOE. - Attempt to add the intermediate CA certificate with the CA Flag configured to FALSE to the TOE's ca-profile. - Verify that the TOE rejects the certificate via log. - Establish the IPsec connection. - Verify via logs that the connection was unsuccessful. - Verify the same via Packet Capture.
Expected Test Results	- The TOE should reject the ICA certificate which has the CA flag set to FALSE. - Evidence (screenshot) showing that the CA flag of the ICA certificate is set to FALSE. - Evidence (screenshot, logs, packet capture) showing unsuccessful IPsec connection.
Pass/Fail with Explanation	Pass. The evaluator has verified that TOE rejected an intermediate CA with the CA flag set to FALSE.

6.108 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	- Verify the status of the Apache server. - Update the CRLs on the TOE. - Host the CRL files on the test VM Apache web server. - Attempt a connection between the TOE and the peer and verify that the connection is successful. - Send traffic through the IPsec tunnel. - Verify that the connection is successful via packet capture. - Make the CRL distribution point unavailable via disabling the CRL server.

	• Remove ICA CRL file from local system-pki directory. • Attempt to establish the IPsec connection. • Attempt to send traffic via the IPsec tunnel. • Verify that the connection is not successful via packet capture. • Verify that the connection is not successful via log.
Expected Test Results	• The TOE should reject the certificates when validation checking of the certificate is not available. • Evidence (screenshot, logs, packet capture) showing unsuccessful IPsec connection.
Pass/Fail with Explanation	Pass. The evaluator manipulated the environment so that the TOE is unable to verify the validity of the certificate, and the TOE rejected the connection.

6.109 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	• Generate a Key. • Verify that the key was successfully generated via logs. • Import the generated key file to the TOE's trust store. • Verify that the key was successfully imported via logs. • Generate a CSR from the TOE. • Verify via logs that the CSR was generated successfully. • Upload the CSR outside the TOE. • Verify the generated CSR and review the claimed contents.
Expected Test Results	Evidence (screenshot, logs) showing generation of CSR with required fields selected in the SFR.
Pass/Fail with Explanation	Pass. The evaluator confirmed that the CSR provides the correct public key and other required information, including any necessary user-input information.

6.110 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	**Part 1** • Generate a key. • Verify that the key was successfully generated via logs. • Import the generated key file to the TOE's trust store. • Verify that the key was successfully imported via logs. • From the TOE, generate a CSR. • Verify via logs that the CSR was generated successfully. • Upload the CSR outside the TOE. • Verify the generated CSR and review the claimed contents. • Generate a signed certificate based on the generated CSR from an external CA. • Import the certificate in the TOE's trust store. • Display the chain of certificates. • Configure the ca-profile on the TOE. • Remove an intermediate certificate from the TOE's trust store. • Re-enable the ca-profile. • Show relevant logs. • Attempt to establish the connection and verify that it fails. • Send traffic to go through the tunnel. • Verify via logs that the connection fails. • Verify via packet capture that the connection fails. • Put some other ICA certificate in the ca-profile. • Show relevant logs. • Attempt to establish the connection and verify that it fails. • Send traffic through the tunnel. • Verify via logs. • Verify via packet capture. **Part 2**

	• Import the ICA in the trust store. • Relevant logs. • Re-enable the ca-profiles. • Show relevant logs. • Verify that the connection is being established. • Send traffic through the IPsec tunnel. • Verify that the connection is established via packet capture. • Add the correct ICA certificate back in the ca-profile. • Show relevant logs. • Verify that the connection is established successfully. • Send traffic through the IPsec tunnel. • Verify the same via packet capture.
Expected Test Results	• The TOE should not validate a signed CSR if the full trust chain is not present. When a full trust chain is present, the TOE should validate the signed CSR. • Evidence (screenshot or CLI output) showing generation of CSR. • CLI output showing successful signing of CSR. • CLI output showing unsuccessful signing of CSR when the trust point is removed.
Pass/Fail with Explanation	Pass. The TOE does not install CSR responses signed by a CA without a full trust path. The TOE installs a CSR response signed by a CA with a full trust path. This meets the testing 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 sections from each AGD were used to determine the verdict of this assurance activity. The AGD specifies that the platforms supported are:

Components	Required (Y/N)	Usage
Local Management Station	Yes	A management station connected to the TOE from the console used for administering the TOE locally.
Remote Management Station	Yes	A management station connected to the TOE over a network connection, used for administering the TOE remotely over SSH.
SSH Client	Yes	The Remote Management Station must run an SSH client which the remote administrator may use for establishing a secure connection between the Remote Management Station and the TOE.

<table>
<tr><td></td><td>
<table>
<tr><td>CA/CRL Server</td><td>Yes</td><td>A server with a certification authority and certificate revocation list used by the TOE for validating the X.509 certificates used for IKE and IPsec connection establishment.</td></tr>
<tr><td>AAA Server</td><td>Yes</td><td>A server implementing RADIUS and TACACS+ which the TOE may be configured to use for external authentication of users.</td></tr>
<tr><td>Syslog Server</td><td>Yes</td><td>A Server to which the TOE may be configured to forward audit log files.</td></tr>
<tr><td>Update Server</td><td>Yes</td><td>A Server hosting the TOE Software Upgrades. The Administrator may connect to the server and download upgrades for the TOE Software.</td></tr>
</table>
Based on these findings, this assurance activity is considered satisfied.
</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

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 set of official guidance documents were used to determine the verdict of this work unit. Each confirmation command indicates tested options. Additionally, the section titled '**Common Criteria Evaluated Configuration'**, sub-section '**Product functionality not included in the scope of the evaluation'**, in the guidance document titled '**NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide'** 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 Test #3. The evaluator verified the guidance documentation describes the process for verifying updates in FPT_TUD_EXT.1 Guidance 2. The evaluator verified the guidance documentation makes it clear which security functionality is covered by the Evaluation Activities in AGD_OPE.1 Test #4. 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

<table>
<tr><td>Objective</td><td>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).</td></tr>
<tr><td>Evaluator Findings</td><td>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 the sections in each of the AGDs. The evaluator found that these sections describe how the Operational Environment must meet:
<table>
<tr><th>Components</th><th>Required (Y/N)</th><th>Usage</th></tr>
<tr><td>Local Management Station</td><td>Yes</td><td>A management station connected to the TOE from the console used for administering the TOE locally.</td></tr>
<tr><td>Remote Management Station</td><td>Yes</td><td>A management station connected to the TOE over a network connection, used for administering the TOE remotely over SSH.</td></tr>
<tr><td>SSH Client</td><td>Yes</td><td>The Remote Management Station must run an SSH client which the remote administrator may use for establishing a secure connection between the Remote Management Station and the TOE.</td></tr>
<tr><td>CA/CRL Server</td><td>Yes</td><td>A server with a certification authority and certificate revocation list used by the TOE for validating the X.509 certificates used for IKE and IPsec connection establishment.</td></tr>
<tr><td>AAA Server</td><td>Yes</td><td>A server implementing RADIUS and TACACS+ which the TOE may be configured to use for external authentication of users.</td></tr>
<tr><td>Syslog Server</td><td>Yes</td><td>A Server to which the TOE may be configured to forward audit log files.</td></tr>
<tr><td>Update Server</td><td>Yes</td><td>A Server hosting the TOE Software Upgrades. The Administrator may connect to the server and download upgrades for the TOE Software.</td></tr>
</table>
Based on these findings, this assurance activity is considered satisfied.</td></tr>
<tr><td>Verdict</td><td>Pass</td></tr>
</table>

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, including,

Components	Required (Y/N)	Usage
Local Management Station	Yes	A management station connected to the TOE from the console used for administering the TOE locally.
Remote Management Station	Yes	A management station connected to the TOE over a network connection, used for administering the TOE remotely over SSH.
SSH Client	Yes	The Remote Management Station must run an SSH client which the remote administrator may use for establishing a secure connection between the Remote Management Station and the TOE.
CA/CRL Server	Yes	A server with a certification authority and certificate revocation list used by the TOE for validating the X.509 certificates used for IKE and IPsec connection establishment.
AAA Server	Yes	A server implementing RADIUS and TACACS+ which the TOE may be configured to use for external authentication of users.
Syslog Server	Yes	A Server to which the TOE may be configured to forward audit log files.
Update Server	Yes	A Server hosting the TOE Software Upgrades. The Administrator may connect to the server and download upgrades for the TOE Software.

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** ○ *Section titled '5.4 Accessing the CLI', '6.13.2.2.1 System Administration Commands', '3.10.2.1.15 Login Control Commands' and '3.10.2.1.6 Password Commands'* • **Configuring SSH and Console Connections** ○ *Section titled '3.10.2.1.13 SSH Commands'* • **Configuring the Remote Syslog Server** ○ *Sections titled '5.2.6 Syslog', '5.10.7 Configuring a Syslog Target', '5.11 Log Management Tasks', '5.11.5 Modifying a Syslog ID' and '5.11.6 Deleting a Syslog ID'* • **Configuring Audit Log Options** ○ *Sections titled '5.2 Log Destinations', '5.6 Configuring Logging with CLI', '5.12 Log Command Reference' and '5.12.2.1 Configuration Commands'* • **Configuring VPNs (IPsec)** ○ *Section titled '8.10.2.1 IPSec Configuration Commands'* 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 Test #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 titled **3.10.2.1.13 SSH Commands** and **3.10.2.1.6 Password Commands** were used to determine the verdict of this work unit. The AGD titled **System Management Guide** 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/view/vuln.search • https://www.nokia.com/ • https://www.suse.com/ • https://www.nokia.com/about-us/security-and-privacy/product-security-advisory/ • https://www.openssl.org/news/vulnerabilities.html The evaluator performed the public domain vulnerability searches using the following key words: • Nokia 7705 SAR • Nokia Service Aggregation Router • Nokia OS 21.10R5 • OpenSSL 1.1.1g • OpenSSH 3.5p1 • Cavium OCTEON Plus • Cavium OCTEON II • Winpath 3 • Winpath • strongSwan 5.5.0 The vulnerability search was performed on 15th September 2023. No open vulnerabilities applicable to the TOE were identified. 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) ▪ mutated packets carrying each ‘Transport Layer Protocol’ value that is undefined in the respective RFC for IPv4 (RFC 791) 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 CAVP Mapping

8.1 Operational Environment of the Algorithm Implementation

This section presents a detailed listing of each algorithm listing to include the name and the OE.

Algorithm	Cert #	Name	Operating Environment
AES	C2023	Nokia 7705 SAR OS Cryptographic library	Cavium OCTEON II CN6335, CN6640 and CN6020
	C2024	Nokia 7705 SAR OS Cryptographic library	Cavium Octeon Plus CN5640, CN5010 and CN5020
SHS	C2023	Nokia 7705 SAR OS Cryptographic library	Cavium OCTEON II CN6335, CN6640 and CN6020
	C2024	Nokia 7705 SAR OS Cryptographic library	Cavium Octeon Plus CN5640, CN5010 and CN5020
HMAC	C2023	Nokia 7705 SAR OS Cryptographic library	Cavium OCTEON II CN6335, CN6640 and CN6020
	C2024	Nokia 7705 SAR OS Cryptographic library	Cavium Octeon Plus CN5640, CN5010 and CN5020
DRBG	C2023	Nokia 7705 SAR OS Cryptographic library	Cavium OCTEON II CN6335, CN6640 and CN6020
	C2024	Nokia 7705 SAR OS Cryptographic library	Cavium Octeon Plus CN5640, CN5010 and CN5020
RSA	C2023	Nokia 7705 SAR OS Cryptographic library	Cavium OCTEON II CN6335, CN6640 and CN6020
	C2024	Nokia 7705 SAR OS Cryptographic library	Cavium Octeon Plus CN5640, CN5010 and CN5020
KAS FFC SSC	A3134	Nokia 7705 SAR OS Cryptographic library	Cavium OCTEON II CN6335, CN6640 and CN6020
	A3133	Nokia 7705 SAR OS Cryptographic library	Cavium Octeon Plus CN5640, CN5010 and CN5020

8.2 SFR to CAVP Mapping

This section provides a table that lists all SFRs for which a CAVP certificate is claimed, the CAVP algorithm list name and the CAVP Certificate number.

SFR	**Algorithm in ST**	**Implementation name**	**CAVP Alg.**	**CAVP Cert #**
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS	Nokia 7705 SAR OS Cryptographic library	RSA KeyGen (FIPS186-4)	C2023

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	PUB 186-4, “Digital Signature Standard (DSS)”, Appendix B.3	Nokia 7705 SAR OS Cryptographic library	RSA KeyGen (FIPS186-4)	C2024
	FFC Schemes using ‘safe-prime’ groups that meet the following: “NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526]	Nokia 7705 SAR OS Cryptographic library	Safe Primes Key Generation Safe Primes Key Verification	A3133
		Nokia 7705 SAR OS Cryptographic library	Safe Primes Key Generation Safe Primes Key Verification	A3134
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”	Nokia 7705 SAR OS Cryptographic library	None	CCTL tested as per the PP/SD Evaluation Activities
	FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800- 56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526]	Nokia 7705 SAR OS Cryptographic library	KAS-FFC-SSC Sp800-56Ar3	A3133
		Nokia 7705 SAR OS Cryptographic library	KAS-FFC-SSC Sp800-56Ar3	A3134
FCS_COP.1/ DataEncryption	AES used in [CBC, CTR] mode and cryptographic key sizes [128 bits, 192 bits, 256 bits]	Nokia 7705 SAR OS Cryptographic library	AES-CBC AES-CTR	C2023
		Nokia 7705 SAR OS Cryptographic library	AES-CBC AES-CTR	C2024

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Nokia 7705 SAR OS Cryptographic library	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4)	C2023
		Nokia 7705 SAR OS Cryptographic library	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4)	C2024
FCS_COP.1/ Hash	[SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits	Nokia 7705 SAR OS Cryptographic library	SHS	C2023
		Nokia 7705 SAR OS Cryptographic library	SHS	C2024
FCS_COP.1/ KeyedHash	[HMAC-SHA-1, HMAC-SHA- 256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [160-bits, 256-bits, 384-bits, 512-bits] and message digest sizes [160, 256, 384, 512] bits	Nokia 7705 SAR OS Cryptographic library	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	C2023
		Nokia 7705 SAR OS Cryptographic library	HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-384 HMAC-SHA-512	C2024
FCS_RBG_EXT.1	CTR_DRBG (AES)	Nokia 7705 SAR OS Cryptographic library	Counter DRBG	C2023
		Nokia 7705 SAR OS Cryptographic library	Counter DRBG	C2024

9 Conclusion

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

End of Document