Nokia 7x50 SR OS 20.10.R12 for 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-a4, and 7750 SR-a8 with maxp10-10/1Gb-msec-sfp + and me12-10/1gb-sfp+ MDAs Guidance Document

Document Version: 0.8

Date: May 30, 2023

intertek acumen security

2400 Research Blvd
Suite 395
Rockville, MD 20850

Contents

1 Overview

This document is intended to be a guidance document to the Nokia 7x50 SR OS 20.10.R12. This Common Criteria guidance document contains configuration information needed to configure and administer the Nokia 7x50 SR OS 20.10.R12. The Nokia 7x50 SR OS 20.10.R12 conforms to the Common Criteria Network Device Protection Profile v2.2e and Network Device collaborative Protection Profile (NDcPP) Extended Package MACsec Ethernet Encryption, Version 1.2 [MACsec v1.2]. The information contained in this document is intended for Administrators who would be responsible for the configuration and management of the Nokia 7x50 SR OS 20.10.R12.

1.1 TOE Overview

The Nokia 7x50 SR OS 20.10.R12 for 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-a4, and 7750 SR-a8 with maxp10-10/1Gb-msec-sfp+ and me12-10/1gb-sfp+ MDAs (herein referred to as the TOE) is a network device with the high-performance, scale and flexibility supporting service providers, web scale and enterprise networks. The Nokia 7x50 routers utilize the Nokia's SR OS technology.

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

1.2 TOE Product Type

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

1.3 TOE Description

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

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

The TOE also supports MACsec functionality between compatible Nokia MACsec peer devices using the Media Dependent Adapter (MDA). The TOE permits only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType is 88-08) and discards others.

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

- Routers 7750 SR-a4 and 7750 SR-a8 support 10-port 10/1GE MACsec MDA maxp10-10/1Gb-msec-sfp+
- Routers 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-7, 7750 SR-12 and 7750 SR-12e support MDA me12-10/1gb-sfp+.

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

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

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

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

The TOE is comprised of the following models as indicated in the table below:

Table 1 – TOE Physical Boundary Components

Platform Description	Processors	MACsec MDA
7750 SR-7 # of Cores: 10 Core Frequency: 1.5Ghz OS: Nokia SR OS Image Version: 20.10.R12 Part number: 3HE08423AA	Cavium OCTEON II CN6645	me12-10/1gb-sfp+

Platform Description	Processors	MACsec MDA
7750 SR-12 # of Cores: 10 Core Frequency: 1.5Ghz OS: Nokia SR OS Image Version: 20.10.R12 Part number: 3HE08423AA	Cavium OCTEON II CN6645	me12-10/1gb-sfp+
7750 SR-12e # of Cores: 10 Core Frequency: 1.5Ghz OS: Nokia SR OS Image Version: 20.10.R12 Part number: 3HE08423AA	Cavium OCTEON II CN6645	me12-10/1gb-sfp+
7750 SR-1e # of Cores: 10 Core Frequency: 1.3Ghz OS: Nokia SR OS Image Version: 20.10.R12 Part number: 3HE10301AA	Cavium OCTEON II CN6645	me12-10/1gb-sfp+

Platform Description	Processors	MACsec MDA
7750 SR-2e # of Cores: 10 Core Frequency: 1.3Ghz OS: Nokia SR OS Image Version: 20.10.R12 Part number: 3HE10302AA	Cavium OCTEON II CN6645	me12-10/1gb-sfp+
7750 SR-3e # of Cores: 10 Core Frequency: 1.3Ghz OS: Nokia SR OS Image Version: 20.10.R12 Part number: 3HE10303AA	Cavium OCTEON II CN6645	me12-10/1gb-sfp+
7750 SR-a4 # of Cores: 6 Core Frequency: 800Mhz OS: Nokia SR OS Image Version: 20.10.R12 Part number: 3HE09195AA	Cavium OCTEON II CN6635	maxp10-10/1Gb-msec-sfp+

Platform Description	Processors	MACsec MDA
7750 SR-a8 # of Cores: 6 Core Frequency: 800Mhz OS: Nokia SR OS Image Version: 20.10.R12 Part number: 3HE09196AA	Cavium OCTEON II CN6635	maxp10-10/1Gb-msec-sfp+

Figure 1 depicts the TOE boundary:

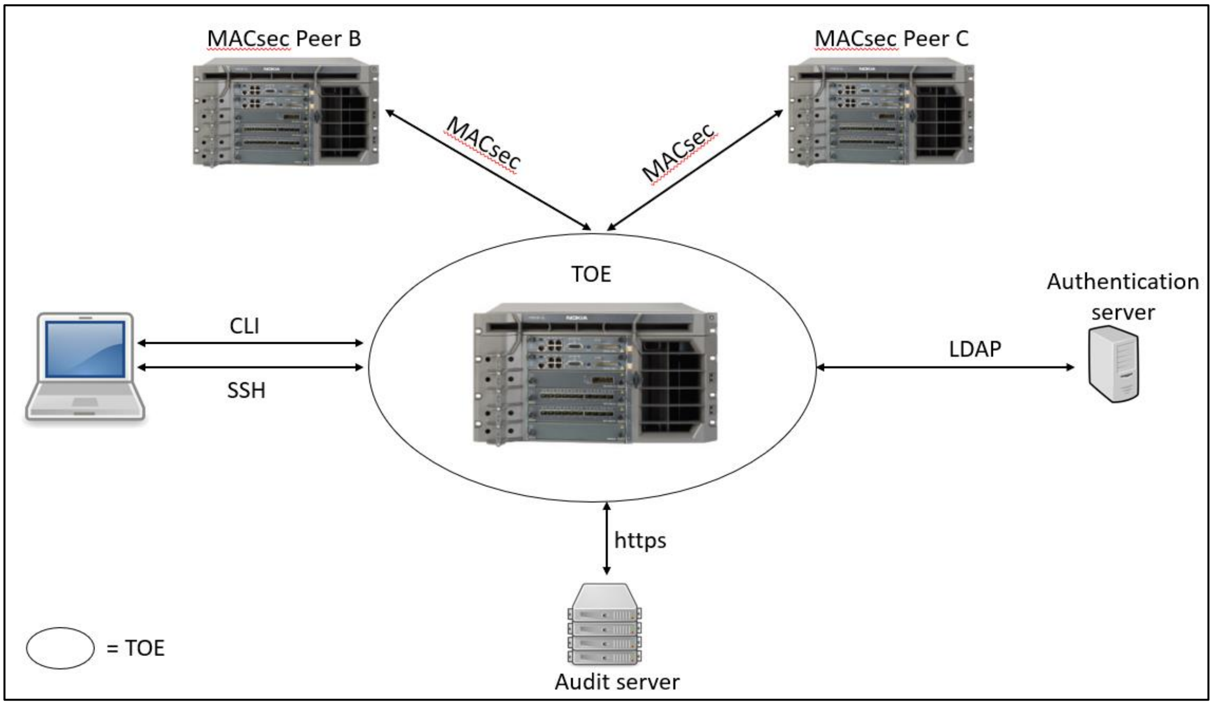

Figure 1 – TOE Boundary Diagram

1.4 Assumptions

The Assumptions included in Table are drawn directly from the PP and any relevant EPs/Modules/Packages.

Table 2 – Assumptions

ID	Assumption
A.PHYSICAL_PROTECTION	The Network Device is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device's physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains. As a result, the cPP does not include any requirements on physical tamper protection or other physical attack mitigations. The cPP does not expect the product to defend against physical access to the device that allows unauthorized entities to extract data, bypass other controls, or otherwise manipulate the device. For vNDs, this assumption applies to the physical platform on which the VM runs.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general-purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality). In the case of vNDs, the VS is considered part of the TOE with only one vND instance for each physical hardware platform. The exception being where components of the distributed TOE run inside more than one virtual machine (VM) on a single VS. There are no other guest VMs on the physical platform providing non-Network Device functionality.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic Network Device does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the Network Device to protect data that originates on or is destined to the device itself, to include administrative data and audit data. Traffic that is traversing the Network Device, destined for another network entity, is not covered by the ND cPP. It is assumed that this protection will be covered by cPPs and PP-Modules for particular types of Network Devices (e.g., firewall).

ID	Assumption
A.TRUSTED_ADMINISTRATOR	The Security Administrator(s) for the network device are assumed to be trusted and to act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The network device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device. For TOEs supporting X.509v3 certificate-based authentication, the Security Administrator(s) are expected to fully validate (e.g. offline verification) any CA certificate (root CA certificate or intermediate CA certificate) loaded into the TOE's trust store (aka 'root store', ' trusted CA Key Store', or similar) as a trust anchor prior to use (e.g., offline verification).
A.REGULAR_UPDATES	The network device firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
A.ADMIN_CREDENTIALS_SECURE	The administrator's credentials (private key) used to access the network device are protected by the platform on which they reside.
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g., cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.

1.5 TOE Evaluated Configuration

In the evaluated configuration, the TOE consists of the platform as stated in Section 1.3. The TOE supports secure connectivity with another IT environment device as stated in Table 3.

Table 1 – IT Environment Components

Components	Required (Y/N)	Usage
Audit server	Yes	The audit server supports HTTP PUT requests over TLS v1.2 to receive audit files securely from the TOE.
LDAP server	Yes	This server will provide the authentication mechanism to authenticate users.
MACsec peer	Yes	This peer is required to test the MACsec functionality.
Management workstation with Web Browser/SSH client	Yes	This includes any IT Environment Management workstation with a Web Browser and an SSH client.
Certificate Authority server	Yes	The Certificate Authority server is used for creation and management of X509 certificates to be used with the TOE.

1.6 TOE Delivery

The TOE is delivered via commercial carrier (i.e. FedEx, UPS, Expeditors etc.). The TOE will contain a packing slip with the serial numbers of all shipped devices. The receiver must verify that the hardware serial numbers match the serial numbers listed in the packing slip. The TOE is shipped with the software pre-installed on it. Software updates are available for download from the Nokia website. When software updates are available via the https://www.nokia.com/ website, customers can obtain, verify the hash integrity and install the updates.

2 Logging into the TOE using local console and SSH

Before beginning this procedure, ensure that:

1. The Nokia 7x50 SR OS 20.10.R12 node has been installed and provisioned with an IP address and gateway for the management network interface. The node (TOE) must be connected to the management network.
2. A terminal emulator application (for example, PuTTY) has been installed on your PC, and the terminal emulator is running.

2.1 Local Console Access:

An authorized administrator requires the following to establish a console connection:

- An ASCII terminal or a PC running terminal emulation software with baud rate of 115,200.
- A standard serial cable with a male DB

This interface is available locally even when other methods of remote access are down. The local console access is subject to administrator lockouts.

1. Connect to the device using local console cable provided in shipping box
2. After powering on the device, wait for the local prompt to appear on the screen.
3. Enter the username of the default user account: **admin**
4. Enter default password of the default user account: **admin**
5. To modify the default password setting, run the following command:

```
*A:SR-xx# configure system security user admin password
<password>
```

Note*: The plaintext password length cannot be more than 56 characters.*

6. To set the minimum password length of six (6), use the following command:

```
*A:SR-xx# configure system security password complexity-rules
minimum-length 6
```

Note: *The TOE does not reveal authentication data while logging into the TOE.*

7. Assign a name to the device using the following command:

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

8. Assign the IP address to the management interface using the following command:

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

2.2 SSH access:

1. Open the terminal emulator on your PC. Specify the IP address of the TOE that you want to connect. If this is the first time anyone has connected to the TOE from a terminal using SSH, you are prompted to add the TOE to your known hosts list.

2. Enter the username of the default user account: `<username>`

3. Enter password of the default user account: `<password>`

Note: *The TOE units have one factory-set user account: admin (root account).*

3 Enabling the FIPS-140-2

The TOE must run in FIPS mode. The 7750 SR includes a configurable parameter in the bof.cfg file to make the node run in FIPS-140-2 mode. When the node boots in FIPS-140-2 mode, the following behaviors are enabled on the node.

To support FIPS-140-2, an HMAC-SHA-256 integrity check is performed to verify the integrity of the software images. The following file is included in the TIMOS-m.n.Yz software bundle containing the hmac-sha-256 signature: hmac-sha256.txt. The node limits the use of encryption and authentication algorithms to only those allowed for the associated FIPS-140-2 certification of the 7750-SR.

When configuring user-defined encryption or authentication keys, CLI will prompt for the key to be re-entered. If the re-entered key does not match the original, the CLI command will be canceled. This affects several protocols and applications.

3.1 Enable FIPS-140-2

Enabling FIPS-140-2 restricts the ability to configure and use cryptographic algorithms and functions that are not FIPS approved. FIPS-140-2 impacts the ability to configure SSH, SNMP and certificates. Please refer to the System Management guide for details on FIPS-140-2 related items.

3.1.1 To enable FIPS-140-2 at the console, follow the steps below:

```
*A:SR-xx# bof fips-140-2

*A:SR-xx# bof save
```

Reboot the device to enable the FIPS mode.

```
*A:SR-xx# admin reboot now
```

3.2 Self-Test

Cryptographic module startup tests are executed on the CPM when the node boots to ensure the associated approved FIPS-140-2 algorithms are operating correctly.

Cryptographic module conditional tests are executed when required during normal operation of associated when using FIPS-140-2 approved algorithms.

3.2.1 Cryptographic POST

1. Manually pull the power cable from the TOE
2. Plug back-in the power cable to the TOE

Note*: The TOE runs the power-on process and must display "FIPS-140-2 Power-On-Self-Test Passed" after the completion of the restart.*

3.2.2 Cryptographic POST

POST is run every time the CPM is rebooted. To reboot the device,

```
*A:SR-xx# admin reboot now
```

Note*: The TOE runs the power-on process and must display "FIPS-140-2 Power-On-Self-Test Passed" after the completion of the reboot.*

3.3 HMAC-SHA-256 integrity check

During the loading of the cpm.tim or both.tim, an HMAC-SHA-256 check is performed to ensure that the calculated HMAC-SHA-256 of the loaded image matches to that stored in the hmac-sha1.txt file.

The HMAC-SHA-256 check is performed on the data loaded from the .tim file. Note that when configuring the primary-image, secondary-image and tertiary-image, the hmac-sha256.txt file must exist in the same directory as the .tim files. If the load has been verified correctly from the HMAC-SHA-256 integrity check, the load continues to bootup as normal. If the load is not verified by the HMAC-SHA-256 integrity check, the image load will fail.

3.3.1 The TOE displays a successful match as below:

```
FIPS-140-2 HMAC-SHA256 software load verification passed
```

After the HMAC-SHA-256 integrity check passes, the node continues its normal bootup 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 in FIPS-140-2 mode. If such configuration is present in the config.cfg file when the node boots, the node will load the config.cfg file until the location of the offending configuration and then halt the configuration at that point. Upon a failure to load the config.cfg file, a failure message is printed on the console.

3.3.2 The FIPS Power on self-test should pass successfully. Upon successful self-test cycle, the TOE should display the following result:

```
FIPS-140-2 Power-On Self-Test started

FIPS-140-2 Power-On Self-Test passed
```

***Note**: If the POST fails, the TOE ceases operation. During this state no one can login, no traffic is passed, the TOE is not operational. If the problem is not corrected by the reboot, please contact Nokia technical assistance.*

3.4 Configuring SSH Rekey

The TOE restricts the ability to manage SSH (session keys) to security administrators via command line. The TOE is capable of rekeying. The TOE verifies the following thresholds:

- No longer than one hour
- No more than 1 GB of transmitted data

The TOE continuously checks both conditions. When either of the conditions are met, the TOE will initiate a rekey.

3.4.1 To set the SSH rekey thresholds value, login as an authorized Security Administrator, and follow the steps below:

```
*A:SR-xx# configure system security ssh key-re-exchange server
minutes <minutes> no shutdown
```

***Note**: The TOE default data transmit size is 1 GB.*

3.5 SNMP Configuration

3.5.1 In the evaluated configuration, SNMP should be disabled (shutdown in configuration). To ensure SNMP service is disabled, run the following command:

```
*A:SR-xx# configure system snmp

*A:SR-xx# >config>system>snmp# info

-----------------------------------------------

            shutdown

-----------------------------------------------
```

3.5.2 To disable the SNMP, run the following command:

```
A:SR-xx# configure system snmp

*A:SR-xx >config>system>snmp# shutdown
```

To save the configuration, use the command below:

```
*A:SR-xx >config>system>snmp# /admin save
```

4 Using an Audit Server

Use the following procedure to configure an audit server.

4.1 Prerequisites

Configure an audit server on external IT environment.

4.2 Audit Server Requirements

The TOE requires an HTTPS server such as NGINX or Apache. The TOE is capable of exporting audit logs to the external audit server using HTTP PUT requests over TLS v1.2 protocol.

4.3 Configure TOE to communicate with an Audit Server

For the TOE to successfully create a log file, the compact flash disk must have a minimum of 10% or 5MB of free space. The TOE is designed to store 6.8 GB records in compact flash drive. When the storage space for audit data is full, the TOE will overwrite the oldest log file.

A cron script can be executed on the TOE to periodically transfer the log files from local storage to the external audit server. The TOE performs the transmission of logs periodically using a cron script. The cron script includes a URL of the external audit sever. The TOE can rollover from one log file to the next log file based on rollover time.

To use an audit server using trusted channel, follow the steps below:

4.3.1 Create a cron script file using vi editor on the TOE:

```
*A:SR-xx# /file vi <local-url>
```

4.3.2 Enter the following text:

```
file copy cf3:/log/* https://a.b.c.d/rw/ force client-tls-
profile "client_tls_prof1"
```

4.3.3 To save the script, run the following command:

```
Press [Esc] key followed by the colon (:), press [w] and hit [Enter]
```

4.3.4 To create script control, run the following command:

```
*A:SR-xx# config>system# script-control

*A:SR-xx >config>system>script-control# script <script-name>

*A:SR-xx >config>system>script-control>script# location "cf3:/filename"

*A:SR-xx >config>system>script-control>script# no shutdown

*A:SR-xx >config>system>script-control# script-policy <policy-name>

*A:SR-xx >config>system>script-control>script-policy# results <file-url>

*A:SR-xx >config>system>script-control>script-policy# script <script-name>

*A:SR-xx >config>system>script-control>script-policy# no shutdown
```

4.3.5 To create a cron job, run the following command:

```
*A:SR-xx >config>system>cron# schedule <schedule-name>

*A:SR-xx >config>system>cron>sched# interval <seconds>

*A:SR-xx >config>system>cron>sched# count <number>

*A:SR-xx >config>system>cron>sched# script-policy <script-policy-name>

*A:SR-xx >config>system>cron>sched# no shutdown
```

If the TLS connections used by the TOE is unintentionally broken, the security administrator needs to restart the connection, or the TOE will try to rejoin with the audit server.

4.4 Auditable Events

4.4.1 Format

The TOE generates a comprehensive set of audit logs that identify specific TOE operations whenever an auditable event occurs. Auditable events are specified in Table 5. Each audit record contains the date and time of event, type of event, subject identity, and the outcome (success or failure) of the event.

All configuration changes are recorded with subject identity as the user request is made through the command line interface (CLI) with either local or remote connection.

4.4.2 NDcPP and MACsec Audit Events

Table 4 NDcPP + MACsec Audit Events

Requirement	Auditable Events	Additional Audit Record Contents	Sample Audit Records
FAU_GEN.1	None	None	
FAU_GEN.2	None	None	
FAU_STG_EXT.1	None	None	
FAU_STG.1	None	None	
FCS_CKM.1	None	None	
FCS_CKM.2	None	None	
FCS_CKM.4	None	None	
FCS_COP.1/DataEncryption	None	None	
FCS_COP.1/SigGen	None	None	
FCS_COP.1/Hash	None	None	
FCS_COP.1/KeyedHash	None	None	
FCS_COP.1(1)/KeyedHashCMAC	None.	None.	
FCS_COP.1/MACsec	None.	None.	
FCS_RBG_EXT.1	None	None	
FCS_TLSC_EXT.2	None	None	
FCS_TLSC_EXT.1	Failure to establish a TLS Session	Failure to establish a TLS Session	Below listed logs show the failure of TLS session. 240 2020/08/26 04:11:32.176 UTC MINOR: TLS #2003 management tls "TLS session failure for application https client router instance management source address 10.1.9.31 source port 49827 destination address 10.1.1.205 destination port 443 failure reason invalidCertificate" 239 2020/08/26 04:11:32.176 UTC MINOR: SECURITY #2116 Base Cert Verification "HTTPS 10.1.1.205 TLS client_tls_prof1 : Certificate /CN=10.20.30.40 verification failed due to IP address or DNS name of peer does not match certificate" 238 2020/08/26 04:11:31.990 UTC MINOR: TLS #2001 management tls "TLS session initiated for application https client router instance management source address 10.1.9.31 source port 49827 destination address 10.1.1.205 destination port 443 tls state initiating"
FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).	Below listed log represents the failed authentication. 30 2020/09/09 20:49:34.649 UTC MINOR: SECURITY #2011 management admin "User admin from 10.1.1.205 failed authentication"
FIA_PMG_EXT.1	None	None	
FIA_UIA_EXT.1 FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address)	Below listed logs represent the identification and authentication mechanism. 6 2020/09/04 00:18:47.075 UTC MINOR: SECURITY #2001 Base admin "User admin from CONSOLE logged in" 9 2020/09/04 00:33:10.598 UTC MINOR: SECURITY #2011 management admin "User admin from 10.1.1.205 failed authentication"

			1577 2020/09/17 15:00:58.638 UTC MINOR: TLS #2001 management tls "TLS session initiated for application ldap client router instance management source address 10.1.9.31 source port 54880 destination address 10.1.3.80 destination port 389 tls state connected" 1576 2020/09/17 15:00:58.628 UTC MINOR: DEBUG #2001 Base CERTMGR "CERTMGR: Cert Verification LDAP 10.1.3.80 TLS client_tls_prof1: Certificate /CN=10.1.3.80 matched to trust-anchor client-ca0" 1575 2020/09/17 15:00:58.624 UTC MINOR: TLS #2001 management tls "TLS session initiated for application ldap client router instance management source address 10.1.9.31 source port 54880 destination address 10.1.3.80 destination port 389 tls state initiating"
FIA_UAU.7	None	None	
FMT_MOF.1/ManualUpdate)	Any attempt to initiate a manual update	None	Below listed log shows the attempt to initiate a manual update where TOE is looking for new image (20.10.R12) version. Time from clock is FRI MAY 14 19:18:18 2021 UTC Switching serial output to sync mode... done Looking for cf3:/bof.cfg ... OK, reading Contents of Boot Options File on cf3: primary-image cf3:\20.10.R12
FMT_MTD.1/CoreData	None	None	
FMT_SMF.1	All management activities of TSF data	None	Below listed log represents the failed authentication. 30 2020/09/09 20:49:34.649 UTC MINOR: SECURITY #2011 management admin "User admin from 10.1.1.205 failed authentication" Following log shows that time has been changed on the TOE. 716 2020/09/01 17:06:00.000 UTC WARNING: SYSTEM #2001 Base System date/time "Date and time on the system is 2020/09/01 17:06:00" Below listed log shows the attempt to initiate a manual update where TOE is looking for new image (20.10.R12) version. TiMOS BOOT LOADER Acceptable bootrom version; found 0x35, expected

			0x39 Time from clock is FRI MAY 14 19:18:18 2021 UTC Switching serial output to sync mode... done Looking for cf3:/bof.cfg ... OK, reading Contents of Boot Options File on cf3: primary-image cf3:\20.10.R12 Below listed logs represent the identification and authentication mechanism. 6 2020/09/04 00:18:47.075 UTC MINOR: SECURITY #2001 Base admin "User admin from CONSOLE logged in" 9 2020/09/04 00:33:10.598 UTC MINOR: SECURITY #2011 management admin "User admin from 10.1.1.205 failed authentication" 1577 2020/09/17 15:00:58.638 UTC MINOR: TLS #2001 management tls "TLS session initiated for application ldap client router instance management source address 10.1.9.31 source port 54880 destination address 10.1.3.80 destination port 389 tls state connected" Below listed log shows the termination of remote session. 78 2020/09/09 23:32:42.385 UTC MINOR: SECURITY #2010 management admin "User admin from 10.1.1.205 logged out" Below listed log shows the termination of a local interactive session. 96 2020/09/10 00:04:13.843 UTC MINOR: SECURITY #2002 Base admin "User admin from CONSOLE logged out"
FMT_SMR.2	None	None	
FPT_SKP_EXT.1	None	None	
FPT_APW_EXT.1	None	None	
FPT_TST_EXT.1	None	None	
FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure)	None.	Below listed output shows the Initiation of update. TiMOS BOOT LOADER Acceptable bootrom version; found 0x35, expected 0x39 Time from clock is FRI MAY 14 19:18:18 2021 UTC

			Switching serial output to sync mode... done Looking for cf3:/bof.cfg ... OK, reading Contents of Boot Options File on cf3: primary-image cf3:\20.10.R12 primary-config cf3:\config.cfg Below listed output shows the success result of the update. Primary image location: cf3:\20.10.R12 Loading image cf3:\20.10.R12\cpm.tim Version C-20.10.R12, Wed Apr 14 12:34:25 PDT 2021 by builder in /builds/c/2010B/R12/panos/main/sros text:(126327936-->309328896) + data:(19302144-->130691904) FIPS-140-2 HMAC-SHA256 software load verification passed Executing TiMOS image at 0x2800000 Total Memory: 4GB Chassis Type: 0x17 Card Type: 0x6e TiMOS-C-20.10.R12 cpm/hops64 Nokia 7750 SR Copyright (c) 2000-2021 Nokia. All rights reserved. All use subject to applicable license agreements. Built on Wed Apr 14 12:34:25 PDT 2021 by builder in / builds/c/2010B/R12/panos/main/sros
FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).	Following log shows that time has been changed on the TOE. 716 2020/09/01 17:06:00.000 UTC WARNING: SYSTEM #2001 Base System date/time "Date and time on the system is 2020/09/01 17:06:00"
FTA_SSL_EXT.1 (if "terminate the session is selected)	The termination of a local interactive session by the session locking mechanism.	None.	Below listed log shows the termination of a local interactive session. 96 2020/09/10 00:04:13.843 UTC MINOR: SECURITY #2002 Base admin "User admin from CONSOLE logged out"
FTA_SSL.3	The termination of a remote session by the	None	Below listed log shows the termination of remote session.

	session locking mechanism.		78 2020/09/09 23:32:42.385 UTC MINOR: SECURITY #2010 management admin "User admin from 10.1.1.205 logged out"
FTA_SSL.4	The termination of an interactive session.	None	Below listed log shows the termination of an interactive session. 1242 2020/09/16 11:34:44.395 UTC MINOR: SECURITY #2002 Base admin "User admin from CONSOLE logged out"
FTA_TAB.1	None	None	
FTP_ITC.1	Initiation of the trusted channel. Termination of the trusted channel. Failure of the trusted channel functions.	Identification of the initiator and target of failed trusted channels establishment attempt.	Below mentioned logs depicts the Initiation of the trusted channel. 1577 2020/09/17 15:00:58.638 UTC MINOR: TLS #2001 management tls "TLS session initiated for application ldap client router instance management source address 10.1.9.31 source port 54880 destination address 10.1.3.80 destination port 389 tls state connected" 1576 2020/09/17 15:00:58.628 UTC MINOR: DEBUG #2001 Base CERTMGR "CERTMGR: Cert Verification LDAP 10.1.3.80 TLS client_tls_prof1: Certificate /CN=10.1.3.80 matched to trust-anchor client-ca0" 1575 2020/09/17 15:00:58.624 UTC MINOR: TLS #2001 management tls "TLS session initiated for application ldap client router instance management source address 10.1.9.31 source port 54880 destination address 10.1.3.80 destination port 389 tls state initiating" Below listed log shows the termination of trusted channel. 98 2020/09/30 00:52:15.035 UTC MINOR: TLS #2002 management tls "TLS session terminated for application ldap client router instance management source address 10.1.9.31 source port 53758 destination address 10.1.3.80 destination port 389" Below listed log shows the failure of trusted channel. 95 2020/09/30 00:52:12.395 UTC MINOR: SECURITY #2003 Base admin "User admin from CONSOLE failed authentication" 94 2020/09/30 00:52:12.395 UTC MINOR: USER #2003 Base admin "User from CONSOLE failed authentication"
FTP_TRP.1/Admin	Initiation of the trusted path. Termination of the trusted path. Failure of the	None.	Below listed logs show an Initiation of the trusted path. 108 2020/09/02 21:37:07.994 UTC MINOR: SECURITY #2009 management admin "User admin from 10.1.1.205 logged in"

	trusted path functions.		107 2020/09/02 21:37:07.994 UTC MINOR: USER #2001 management admin "User from 10.1.1.205 logged in" Below listed logs show Termination of the trusted path. 128 2020/09/02 21:39:22.821 UTC MINOR: SECURITY #2010 management admin "User admin from 10.1.1.205 logged out" 127 2020/09/02 21:39:22.821 UTC MINOR: USER #2002 management admin "User from 10.1.1.205 logged out" Below listed logs show a failure of the trusted path. 118 2020/09/02 21:36:19.402 UTC MINOR: SECURITY #2011 management admin "User admin from 10.1.1.205 failed authentication" 117 2020/09/02 21:36:19.402 UTC MINOR: USER #2003 management admin "User from 10.1.1.205 failed authentication"
FCS_SSHS_EXT.1	Failure to establish an SSH session	Reason for failure	4159 2021/01/22 19:27:38.952 UTC MINOR: SECURITY #2011 management admin "User admin from 10.1.2.166 failed authentication"
FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate Any addition, replacement, or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store	Below mentioned log shows the verification failure. 178 2020/08/25 00:44:26.389 UTC MINOR: SECURITY #2116 Base Cert Verification "HTTPS 10.1.1.205 TLS client_tls_prof1 : Certificate /CN=10.1.1.205 verification failed due to unable to get local issuer certificate - at certificate:/CN=10.1.1.205"
FIA_X509_EXT.2	None	None	
FIA_X509_EXT.3	None	None	
FCS_MACSEC_EXT.1	Session establishment	Secure Channel Identifier (SCI)	Below listed log shows that session was established with Secure Channel Identifier (SCI). 127 2020/07/31 14:00:13.582 UTC MINOR: MACSEC #2006 Base "MACsec MKA session established with MI:SCI bee1d928adb55d8d3698c99a:a47b2ce116150001 on port 1/1/1 sub-port 1 CA NIAP_TOE_128_256_01 EAPOL-destination 01:80:c2:00:00:03 local key-server priority 16 peer key-server priority 16 cipher-suite

			gcm-aes-128 encryption offset 0"
FCS_MACSEC_EXT.1.7	Creation of Connectivity Association	Connectivity Association Key Names	Below mentioned log shows the creation of Connection Association Key Name. 121 2020/07/31 14:00:08.687 UTC MINOR: MACSEC #2011 Base "MACsec CA NIAP_TOE_128_256_01 psk-index 1 CKN ffeeddccbbaa00998877665544332211 created"
FCS_MACSEC_EXT.3.1	Creation and update of Secure Association Key	Creation and update times	Below mentioned log shows the creation of Secure Association Key.
FPT_RPL.1	Detected replay attempt	None	Below listed log shows the replay counts which were detected. 53791 2020/08/06 11:43:25.481 UTC MINOR: MACSEC #2015 Base "MACsec CA NIAP_TOE_128_256_01 port 1/1/1 sub-port 1 MACsec MKA packets replay count 53366" 53790 2020/08/06 11:43:24.470 UTC MINOR: MACSEC #2015 Base "MACsec CA NIAP_TOE_128_256_01 port 1/1/1 sub-port 1 MACsec MKA packets replay count 53365"

5 Configuring MACsec authentication

The TOE restricts the ability to manage and configure the pre-shared key for MACsec functionality to security administrators via command line. The Security Administrator has the ability to configure, modify, and delete the pre-shared key for MACsec functionality.

5.1 Prerequisite:

- Login as an authorized Security Administrator

5.2 Configuring cards and MDAs:

5.2.1 Verify the cards are provisioned.

```
*A:SR-xx# show card
```

5.2.2 If cards are inserted but they are not configured, follow the steps below to configure:

```
*A:SR-xx# /configure card <card number> card-type <type from
inserted card type in the show command output>
```

5.2.3 Verify the modules are provisioned into the card.

```
*A:SR-xx# show mda
```

5.2.4 If mda is plugged in but not configured, follow the steps below to configure:

```
   *A:SR-xx# /configure card <slot-number> mda <mda-slot> mda-type
<mda-type>
```

5.3 Configuring MACsec

The Security Administrator has the ability to configure and manage the MACsec functionality. The TOE authenticates and encrypts frames between itself and MACsec peers. By default, MACsec is disabled and there are no connectivity-association policies configured on Nokia 7x50 SROS. The MACsec connectivity-association (CA) policy needs to be configured first and then this policy has to be linked to a MACsec sub-port configured under a physical port.

The TOE implements an MKA Lifetime Timeout limit of 6 to 18 seconds and a default value for the Hello Timeout limit of 2 sec with Hello Timeout configuration values of 500ms, and 1 to 6 sec. The TOE supports pairwise CAK. The TOE ensures MACsec peer authentication by only using pre-shared keys.

5.3.1 Enabling macsec under a port/subport will ensure any traffic traversing that port/subport will be encrypted via MACsec. Services and interface that are using that port/subport to transmit traffic will be encrypted. As an example, a layer 3 interface can be created using this port/subport via the command:

```
*A:SR-xx# /configure router interface <interface-name> create

*A:SR-xx# /configure router interface <interface-name> address
<ip-address[/mask]>

*A:SR-xx# /configure router interface <interface-name> port
x/y/z
```

Assigning the port/subport of x/y/z with single tag of A

```
*A:SR-xx# /configure router interface <interface-name> create
port x/y/z:A
```

5.3.2 To configure MACsec connectivity association (CA) policy, follow the steps below:

1. Configure the MACsec connectivity-association (ca-name)

```
*A:SR-xx# /configure macsec connectivity-association <ca-name>
create
```

***Note**: This is a MACsec policy which is used by multiple MACsec sub-ports or a single sub-port.*

The TOE should be configured, via authorization methods, so only the Security Administrator has the ability to configure the pre-shared key for MACsec functionality. The TOE ensures MACsec peer authentication by using pre-shared keys. Each of the keys used by MKA is derived from the CAK.

2. Create the pre-shared key (PSK) with the supported encryption type:

```
*A:SR-xx#/configure macsec connectivity-association <ca-name>
static-cak
```

The TOE supports CAK of 32 hex characters for aes-128-cmac encryption algorithm and 64 hex characters for aes-256-cmac encryption algorithm.

```
*A:SR-xx >config>macsec>conn-assoc>static-cak# pre-shared-key
<pre-shared-key index> encryption-type <encryption-type> create
```

***Note:** The pre-shared-key index can be 1 and/or 2. The supported "encryption-type" are aes-128-cmac and aes-256-cmac.*

The TOE supports CAK, which is based on AES cipher in CMAC mode and key sizes of 128 and 256 bits. When the TOE uses AES 128-bit CMAC mode encryption, the supported key size is 32 hexadecimal characters in length. When the TOE uses 256-bit encryption, the supported key size is 64 hexadecimal characters in length and the CAK name (CKN) is a 2 to 64 hexadecimal characters long value.

3. Create the connectivity association key name (CKN) and connectivity association key (CAK):

```
*A:SR-xx >config>macsec>conn-assoc>static-cak>pre-shared-key#
ckn <hex-string>
```

```
*A:SR-xx >config>macsec>conn-assoc>static-cak>pre-shared-key$
cak <hex-string>
```

4. To delete a PSK, run the following command:

```
*A:SR-xx >config>macsec>conn-assoc>static-cak>no pre-shared-key
<pre-shared-key index>
```

5. The default active-psk is 1. For psk rollover to 2, run the following command:

```
*A:SR-xx >config>macsec>conn-assoc>static-cak#active-psk 2
```

6. Configure MKA hello interval

```
*A:SR-xx#/configure macsec connectivity-association "Name of
connectivity association" static-cak mka-hello-interval 500ms
```

***Note**: The available mka-hello- interval values are: 500ms, 1, 2, 3, 4, 5 and 6*

7. Activate the delay -protection on the macsec policy

```
*A:SR-xx#/configure macsec connectivity-association "Name of
connectivity association" delay-protection
```

***Note**: Reply Protection must be enabled before the delay protection*

8. Configure the encryption-offset

```
*A:SR-xx#/configure macsec connectivity-association
"NIAP_TOE_128_256_01" encryption-offset 0
```

***Note**: The available encryption offset values are: 0, 30, and 50*

9. Configure the MKA Key-server-priority

In a mutually authenticated MACsec peers, the TOE can be designated to be a Key Server that distributes the symmetric Secure Association Keys (SAKs). The "mka-key-server-priority" needs to be configured on the TOE and should be of a lower number compared to other peers. This key-server-priority can be configured any number between 0 and 255. The default key-server-priority number is 16. To configure the TOE to be designated as a MKA key-server, run the following command:

```
*A:SR-xx#/configure macsec connectivity-association "Name of
connectivity association" static-cak# mka-key-server-priority
<priority number>
```

10. To activate the MACsec policy, execute “no shutdown” command:

```
*A:SR-xx#/configure macsec connectivity-association no shutdown
```

11. Configure the port and link it to MACsec

```
*A:SR-xx#/configure port <port-id>
```

An SR port is denoted with “slot/mda/port”, where slot is the slot number, mda is the MDA number and port is the port number. An example of port number can 1/2/3 (card 1 mda 2 port 3).

Once the port is configured, to configure macsec ethernet dot1x follow the steps below:

```
*A:SR-xx#/configure port <port-id> ethernet dot1x macsec
```

Here, a number of common macsec attributes can be configured like rx-must-be-encrypted as below:

```
*A:SR-xx#>config>port>ethernet>dot1x>macsec# rx-must-be-
encrypted
```

12. Create the MKA participants

After creating the port, next step is to create the MKA participants to a sub-port under the same configured port. One or multiple macsec sub-ports can be created under port x/y/z. Supports can be created for:

a. Encrypting the entire port including untagged, tagged and double tagged traffic
b. Encrypting only untagged traffic
c. Encrypting only single tag traffic (specific tag, or all single tagged traffic)
d. Encrypting only double tag traffic (specific tags, any outer tag and specific inner tag)

```
*A:SR-xx#/configure port x/y/z ethernet dot1x macsec sub-port <macsec
sub-port id> create
```

After creating the macsec sub-port, configure the following attributes for MKA participant under the sub-port:

```
 *A:SR-xx#/configure port x/y/z ethernet dot1x macsec sub-port
<macsec sub-port id>
*A:SR-xx >config>port>ethernet>dot1x>macsec>sub-port# ca-name
<ca-name>
```

13. Configure the max number of peers supported on this sub-port:

```
*A:SR-xx >config>port>ethernet>dot1x>macsec>sub-port# max-peer
<num-peers>
```

14. Activate the MKA participant:

```
*A:SR-xx#/configure port x/y/z ethernet dot1x macsec sub-port
<macsec sub-port id> no shutdown
```

15. Delete the existing MKA participant:

```
*A:SR-xx#/configure port x/y/z ethernet dot1x macsec sub-port
<macsec sub-port id> no ca-name <ca-name>
```

The pre-shared-key 1 is enabled by default on the TOE. Enabling the pre-shared-key 2 creates new CAK on the key-server. The key-server distributes the new SAK as soon as the MACsec functionality is operational.

16. Enable pre-shared-key 2 (active-psk 2) on the key-server

```
*A:SR-xx#/configure macsec connectivity-association "Name of
connectivity association"

*A:SR-xx >config>macsec>connectivity-association# shutdown

*A:SR-xx >config>macsec>connectivity-association# static-cak

*A:SR-xx >config>macsec>conn-assoc>static-cak> active-psk 2

*A:SR-xx >config>macsec>conn-assoc>static-cak>back

*A:SR-xx >config>macsec>connectivity-association# no shutdown
```

17. Renew CAK/CKN on the key-server

```
*A:SR-xx#/configure macsec connectivity-association "Name of
connectivity association"

*A:SR-xx >config>macsec>connectivity-association# shutdown

*A:SR-xx >config>macsec>connectivity-association# static-cak

*A:SR-xx >config>macsec>conn-assoc>static-cak# pre-shared-key 1

*A:SR-xx >config>macsec>conn-assoc>static-cak>pre-shared-key#
cak <hex-string>

Re-enter key <hex-string> : <hex-string>

*A:SR-xx >config>macsec>conn-assoc>static-cak>pre-shared-key#
ckn <hex-string>

*A:SR-xx >config>macsec>conn-assoc>static-cak>pre-shared-key#
back

*A:SR-xx >config>macsec>conn-assoc>static-cak# back

*A:SR-xx >config>macsec>connectivity-association# no shutdown
```

5.3.3 Specify a lifetime for CAKs

To specify a lifetime for MACsec CAK, create a script, and a cron job for this script. Run the following command to create a script:

```
*A:SR-XX# /file
```

1. Using vi text editor, create a filename for the script

```
*A:SR-XX>file cf3:\ # vi lifetime_for_CAK
```

2. Add the following commands to the newly created script

```
/configure macsec connectivity-association <ca-name> static-cak
active-psk 2
```

3. To save the script, run the following command:

```
Press [Esc] key followed by the colon (:), press [w][q] and hit
[Enter]
```

4. Configure "system script-control" for the newly created script using the commands below:

```
*A:SR-XX# /configure system script-control

*A:SR-XX>config>system>script-control# script "lifetime_for_CAK"

*A:SR-XX>config>system>script-control# shutdown

*A:SR-XX>config>system>script-control# description
specify_lifetime_for_CAK1

*A:SR-XX>config>system>script-control# location
"cf3:/lifetime_for_CAK"

*A:SR-XX>config>system>script-control# no shutdown

*A:SR-XX>config>system>script-control# exit
```

5. Configure "system script-policy" for the newly created script using the commands below:

```
*A:SR-XX# /configure system script-control

*A:SR-XX>config>system>script-control# script-policy
"lifetime_for_CAK"

*A:SR-XX>config>system>script-policy# shutdown

*A:SR-XX>config>system>script-policy# results
"cf3:/results_lifetime_for_CAK "

*A:SR-XX>config>system>script-policy# script "lifetime_for_CAK"

*A:SR-XX>config>system>script-policy# no shutdown

*A:SR-XX>config>system>script-policy# exit
```

6. Configure a cron job for the newly created script using the commands below:

```
*A:SR-XX# /configure system cron

*A:SR-XX>config>system>cron# schedule "lifetime_for_CAK"

*A:SR-XX>config>system>cron>sched# shutdown

*A:SR-XX>config>system>cron>sched# description "specify lifetime
for CAK"

*A:SR-XX>config>system>cron>sched# script-policy
"lifetime_for_CAK"

*A:SR-XX>config>system>cron>sched# type periodic

*A:SR-XX>config>system>cron>sched# interval <seconds>
```

7. Specify the weekday, month, day-of-month, hour, and minute by using the commands below:

```
*A:SR-XX>config>system>cron>sched# weekday <day-name>
```

```
*A:SR-XX>config>system>cron>sched# month <month-name>

*A:SR-XX>config>system>cron>sched# day-of-month <day-number>

*A:SR-XX>config>system>cron>sched# hour <hour-number>

*A:SR-XX>config>system>cron>sched# minute <minute-number>

*A:SR-XX>config>system>cron>sched# no shutdown

*A:SR-XX>config>system>cron>sched# exit
```

8. Save the configuration using the command below:

```
*A:SR-XX># /admin save
```

Note: *NTP server must be configured on all nodes.*

Note: *A second script can be created to switch between the PSK 1 and PSK 2. These two scripts, when used to periodically switch between the PSKs, should be starting at the same time but with interleaved intervals.*

6 Authentication

6.1 Role Based Access Control (RBAC)

The TOE implements Role Based Access Control (RBAC). Security Administrative must login before they can access any administrative functions. The TOE restricts the ability to manage the TOE to Security Administrators. Only administrators can manage the certificates in TOE's trust store. Security Administrators can configure user's privilege that grant or deny privilege to users from login access via Console and Remote access.

For the purpose of the Common Criteria, only the Security Administrator role was tested.

Table 5 Roles and Permissions

Roles	Permissions
Security Administrator	Can configure user accounts and manage users and their associated privileges (member profiles).
	Ability to administer the TOE locally and remotely
	Ability to configure the access banner
	Ability to configure the session inactivity time before session termination or locking
	Ability to update the TOE, and to verify the updates using digital signatures capability prior to installing those updates
	Ability to configure the authentication failure parameters
	Ability to configure audit behavior
	Ability to set the time which is used

Roles	Permissions
	for time-stamps
	Ability to configure the reference identifier for the peer
	Can change their own password, but not other user's passwords

6.1.1 Creating a user account

To create a local user account, use the command:

```
*A:SR-xx# config system security user <user-name>
```

***Note**: The privilege level can be assigned using "console member" command and selecting access level from the available profiles.*

```
*A:SR-xx # config > system > security > user > console member
<user-profile-name>
```

6.1.2 Deleting a user account

To delete a local user account, use the command:

```
*A:SR-xx# config system security no user <user-name>
```

6.2 Password Management

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.

6.2.1 To create a user account and setting of the password use the following command:

```
*A:SR-xx# configure system security user <username>
```

***Note**: The username cannot be more than 32 characters.*

```
*A:SR-xx# configure system security user <username> password
<password>
```

***Note**: The plaintext password length cannot be more than 56 characters.*

6.2.2 To set the minimum password length of six (6), use the following command:

```
*A:SR-xx# configure system security password complexity-rules
minimum-length 6
```

6.3 Configure SSH Public Keys

The TOE restricts the ability to manage SSH (session keys) to security administrators via command line. The Security Administrator has the ability to 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.

6.3.1 Login as an authorized Security Administrator and import the public key for the user. Follow the steps below to set up the public key for SSH user authentication:

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

*A: SR-xx >config>system>security>user# public-keys rsa rsa-key
<rsa-public-key-id> create

*A: SR-xx >config>system>security>user>public-keys>rsa>rsa-key$
key-value <rsa-public-key-value>

Re-enter key <rsa-public-key-value>
```

6.4 Configure X.509 Certificate Authentication for TLS Mutual Authentication

The TOE restricts the ability to manage any configured X.509 certificates (public and private key pairs) to security administrators via command line.

The TOE supports the X.509v3 certificates as defined by RFC 5280 to support authentication of external TLS peers. Only RSA based certificates are supported. The TOE validates the certificates and the extendedKeyUsage field for “TLS Web Server Authentication” and “TLS Web Client Authentication.” 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.

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.

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.

6.4.1 To configure the certificate revocation on the TOE, use the following commands:

```
*A: SR-xx# config system security pki ca-profile <name>
revocation-check crls
```

6.5 Generation of a Certificate Signing Request

The TOE generates a Certificate Request as specified by RFC 2986 and is able to provide the following information in the request: public key and Common Name, Country, Organization, and Organizational Unit.

The TOE validates the chain of certificates from the Root CA upon receiving the CA Certificate Response. The TOE does not support the “device-specific information” within Certificate Request message.

6.5.1 Login as an authorized Security Administrator, and create a keypair using the following command:

```
*A:SR-xx# /admin certificate gen-keypair <url-string> type rsa
size 2048
```

***Note**: The TOE accepts RSA keys of at least 2048 bits up to 8192 bits in key length. The default key size is 2048.*

6.5.2 Once the keypair has been created, run the following commands to create a Certificate Signing Request (CSR):

```
*A:SR-xx# /admin certificate gen-local-cert-req keypair <url-
string> subject-dn CN=<a.b.c.d>,C=<country>,O=<organization
name>,OU=<organizational unit> file <url-string>
```

6.6 Authentication Failure Handling

The Security Administrator can configure the maximum number of failed attempts for the CLI interface. The TOE allows the administrator to configure the number of successive failed authentication attempts within allowed time (in minutes).

```
*A:SR-xx#/configure system security password

*A:SR-xx>config>system>security>password# attempts <count> time
<minutes> lockout <minutes>
```

When a user fails to authenticate a number of times equal to the configured limit, the TOE locks the claimed user identity until the configured time is reached.

Administrators can configure unsuccessful authentication attempts range between 1 – 64 within a configurable time limit of 0 to 60 minutes. When the account is locked, the TOE does not permit any further actions until the account is accessible.

The authentication failures cannot lead to a situation where no administrator access is available. A user would be configured to access the LDAP server which would provide local access to the TOE. The LDAP server is not subject to lockout.

6.7 Logging out of the local CLI and remote SSH interfaces

To facilitate ending a session, the administrative user must log out of the TOE.

6.7.1 Local CLI and remote SSH, use the following command:

```
*A:SR-xx # logout
```

7 Cryptographic Protocols

Enabling CC-NDcPP compliance will ensure that only certified algorithms and key sizes are available for use by the appliance. The TOE restricts the ability to manage SSH (session keys), TLS (session keys), and any configured X.509 certificates (public and private key pairs) to security administrators via command line. The Security Administrator has the ability to configure, modify, generate, and delete the key for SSH.

7.1 SSH

7.1.1 To configure the permissible SSH server cipher algorithm for the system services, login as an authorized Security Administrator, and follow the steps below:

```
*A:SR-xx # /config system security ssh server-cipher-list
protocol-version 2 cipher 190 name aes256-ctr

*A:SR-xx # config > system > security > ssh# server-cipher-list
protocol-version 2 cipher 194 name aes128-ctr

*A:SR-xx # config > system > security > ssh# server-cipher-list
protocol-version 2 cipher 200 name aes128-cbc

*A:SR-xx # config > system > security > ssh# server-cipher-list
protocol-version 2 cipher 230 name aes256-cbc
```

7.1.2 To configure the SSH key-exchange for Diffie-Hellman keys for the system services, login as an authorized Security Administrator, and follow the steps below:

```
*A:SR-xx >config>system>security>ssh>server-kex# kex <index>
name diffie-hellman-group14-sha1

*A:SR-xx >config>system>security>ssh>server-kex# kex <index>
name diffie-hellman-group14-sha256

*A:SR-xx >config>system>security>ssh>server-kex# kex <index>
name diffie-hellman-group16-sha512
```

7.1.3 To configure the allowed message authentication code algorithm for SSHv2 protocol, login as an authorized Security Administrator, and follow the steps below:

```
*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
```

Note*: The TOE only accepts RSA public key.*

7.2 TLS

The TOE restricts the ability to manage TLS (session keys), and any configured X.509 certificates (public and private key pairs) to security administrators via command line.

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.

7.2.1 Prerequisites

Create certificates using available tool which includes Root, Intermediate, Client and Server certificates. Additionally, create CRLs of Root and Intermediate certificates.
Import Root, Intermediate, client certificates and CRL in PEM or DER format to the TOE.
***Note**: Make sure the time on the TOE is in UTC time zone.*

The TOE validates the revocation status of the certificate using a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5. 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.

7.2.2 Login as an authorized Security Administrator, and import Root certificate and CRL using command below:

```
*A:SR-xx # / admin certificate import types cert input
"certificate path with name" output "certificate name" format
der

*A:SR-xx # / admin certificate import type crl input "CRL path
with name" output "CRL name" format der
```

Example:

```
*A:SR-xx # / admin certificate import type cert input
cf1:/client_ca0.cer output client_ca0.cer format der

*A:SR-xx # / admin certificate import type crl input
cf1:/client_ca0.crl output client_ca0.crl format der
```

7.2.3 Login as an authorized Security Administrator, and import Intermediate Root certificate and Intermediate CRL using the command below:

```
A:SR-xx # / admin certificate import type cert input
"certificate path with name" output "certificate name" format
der

*A:SR-xx # / admin certificate import type crl input "CRL path
with name" output "CRL name" format der
```

Example:

```
*A:SR-xx # / admin certificate import type cert input
cf1:/ICA.cer output ICA.cer format der
```

```
*A:SR-xx # / admin certificate import type crl input
cf1:/ICA.crl output ICA.crl format der
```

The TOE validates the extendedKeyUsage field for each certificate as they are presented. The server certificate 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. Similarly, client certificate 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.

7.2.4 Login as an authorized Security Administrator, and import client certificate using the command below:

```
A:SR-xx # / admin certificate import type cert input
"certificate path with name" output "certificate name" format
der validate-cert-chain
```

Example:

```
*A:SR-xx # / admin certificate import type cert input
cf1:/client.cer output client.cer format der validate-cert-chain
```

***Note**: If the TOE is unable to establish a connection to determine the validity of a certificate, the TOE will not accept the certificate.*

7.2.5 To configure "ca-profile" for TLS cert profiles, follow the steps below:

```
A:SR-xx # /configure system security pki ca-profile <name>

*A:SR-xx >config>system>security>pki>ca-profile# cert-file
<filename>

*A:SR-xx >config>system>security>pki>ca-profile# crl-file
<filename>

*A:SR-xx >config>system>security>pki>ca-profile# auto-crl-update

*A:SR-xx >config>system>security>pki> ca-profile# auto-crl-
update# crl-urls url-entry <entry-id>

*A:SR-xx >config>system>security>pki>ca-prof>auto-crl-
update>crl-urls>url-entry# file-transmission-profile <profile-
name>
```

***Note**: The file-transmission-profile needs to be created using commands below:*

```
*A:SR-xx # /config system file-transmission-profile <name>

*A:SR-xx >config>system>security>pki>ca-profile#
```

7.2.6 Configuring a TLS cert prof

```
*A:SR-xx # /configure system security tls cert-profile <profile-
name> create
```

```
*A:SR-xx>config>system>security>tls>cert-profile>entry <entry-id>

*A:SR-xx >config>system>security>tls>cert-profile>entry# cert <cert-filename>

*A:SR-xx >config>system>security>tls>cert-profile>entry# key <key-filename>

*A:SR-xx >config>system>security>tls>cert-profile>entry# send-chain ca-profile <name>
```

***Note**: The ca-profile should be already configured on the TOE PKI settings.*

7.2.7 Configuring a client-cipher-list

```
*A:SR-xx >config>system>security>tls# client-cipher-list  <name>

*A:SR-xx >config>system>security>tls# client-cipher-list> cipher <index> name <cipher-suite-code>
```

***Note**: The TOE allows following tls cipher-suite. Configure the cipher-suite-code for each tls ciphers*

```
tls-rsa-with-aes256-cbc-sha256
tls-rsa-with-aes256-cbc-sha
tls-rsa-with-aes128-cbc-sha256
tls-rsa-with-aes128-cbc-sha
```

***Note**: The TOE supports DNS-ID and CN-ID, IPv4 address in SAN, and IPv6 address in the SAN as a reference identifier and they are enabled on the TOE.*

7.2.8 Configuring a TLS Trust Anchor

```
*A:SR-xx >config>system>security>tls# trust-anchor-profile <name>

*A:SR-xx >config>system>security>tls>trust-anchor-profile# trust-anchor <ca-profile-name>
```

***Note**: Use the ca-profile-name already configured on the section 7.2.4*

7.2.9 Configuring a client TLS profile

```
*A:SR-xx >config>system>security>tls# client-tls-profile <name>

*A:SR-xx >config>system>security>tls>client-tls-profile# cert-profile <name>
```

***Note**: Use the cert-profile already configured on the section 7.2.5*

```
*A:SR-xx >config>system>security>tls>client-tls-profile# cipher-list <name>

*A:SR-xx >config>system>security>tls>client-tls-profile# trust-anchor-profile <name>
```

***Note**: Use the “trust-anchor profile” already configured on the section 7.2.7*

```
*A:SR-xx >config>system>security>tls>client-tls-profile# no
shutdown
```

7.2.10 Activate the “cert-profile”

To activate the cert-profile, execute “no shutdown” command.

```
*A:SR-xx # /configure system security tls cert-profile cert-
profile <name> no shutdown
```

8 Performing Manual Software Updates on the TOE

Customers receive a compact flash with the updated software or are instructed to copy a downloaded image onto a compact flash (received out of band). Customers must log in to Nokia’s secured portal to download software updates, and then copy it onto the compact flash. The compact flash is inserted into the standby CPM and then plugged into the chassis.

The TOE provides means to authenticate firmware updates to the TOE using a published hash prior to installing the firmware. The “hmac-sha256.txt” file is included in the software update bundle that has published hash values.

8.1 Prerequisites

8.1.1 Determine the current version of the TOE by running the following command:

```
 *A:SR-xx# show version
```

***Note**: To perform a manual update, administrator must have a console connection to the TOE. Prior to performing manual software update, confirm all running configuration are saved.*

8.1.2 To save any configuration, run the following the command:

```
*A:SR-xx# /admin save

*A:SR-xx# /bof save
```

8.2 Update the boot options

8.2.1 To update the boot options file (bof) with the new image file, follow the steps below:

```
*A:SR-xx# bof

*A:SR-xx >bof# primary-image cf3:\filename\

*A:SR-xx >bof# save
```

8.3 Reboot the TOE

```
*A:SR-xx# /admin reboot now
```

***Note**: The BOF must be located on the same compact flash drive as the boot.ldr file.*

When the standby CPM boots, it searches for the bootloader in cf3:\ and after finding the boot.ldr, it looks for the file cf3:\bof.cfg

The runtime image attempts to locate the configuration file as configured in the BOF. The first location searched is the primary configuration location. If not found, the secondary configuration location is searched, and lastly, the tertiary configuration location is searched.

Once it detects the standby CPM is operational with the new updated software, then the operator has the option to switchover to the standby CPM running the authenticated software.

***Note**: The administrator must authorize the switchover to the standby CPM within 3 seconds.*

This switchover mechanism provides minimal service interruption during a software upgrade.

8.3.1 To update the settings on the TOE, follow the steps below:

1. Type "sros" and hit ENTER within 22 seconds to begin changing parameters: sros
2. Press ENTER to begin
3. Update the Software Image URL to cf3:\filename\
4. Press ENTER
5. Press ENTER to keep the existing Config URL
6. Enter “no” for IPv4 Autoconfiguration
7. Enter “no” for IPv6 Autoconfiguration
8. Enter “yes” to preserve all existing network settings
9. Enter “yes” to preserve all existing ip network settings
10. Enter “yes” to preserve all existing ipv6 network settings
11. Press ENTER to keep the existing fips-140-2 configuration
12. Enter “no” for Automated-Provisioning
13. Enter “yes” to overwrite cf3:/bof.cfg with the new settings

Once the new config setting is successfully saved, the TOE loads the new image file from the primary-image location.

8.4 HMAC-SHA-256 integrity check

When the standby CPM boots, its bootloader will extract the published hmac-sha256 hash from a file in the compact flash and compare it with the hmac-sha256 hash computed over the new software binary. If the hashes match, then it will "jump" into or run the new software binary. Otherwise, it will show a FIPS HMAC-SHA256 error on the console, reboot and repeat the cycle. Meanwhile, the active CPM in the same chassis is still running the current software.

8.4.1 The TOE displays a successful match as below:

```
FIPS-140-2 HMAC-SHA256 software load verification passed
```

With every firmware update, the FIPS Power on self-test should pass successfully.

8.5 Self-Test

Cryptographic module startup tests are executed on the CPM when the node boots to ensure the associated approved FIPS-140-2 algorithms are operating correctly.

8.5.1 Upon successful self-test cycle, the TOE displays following result:

```
FIPS-140-2 Power-On Self-Test started

FIPS-140-2 Power-On Self-Test passed
```

8.6 Updated Image Version

8.6.1 After the successful completion of the image update, login as an authorized Security Administrator and check the image version as below:

```
 *A:SR-xx# show version
```

9 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,

9.1.1 Set the system time

```
*A:SR-xx# admin set-time <YYYY/MM/DD>
```

9.1.2 Confirm the system time and date:

```
*A:SR-xx# show time
```

9.1.3 Save the provisioned setting to the configuration file:

```
*A:SR-xx# /admin save
```

10 Automatic Logout due to Session Inactivity

A Security Administrator can configure maximum inactivity times for administrative sessions through the TOE local console CLI and remote SSH CLI interfaces. The default value is 30 minutes for the local console CLI and remote SSH CLI interfaces. The configuration of inactivity periods is a global parameter for the chassis, and it get applied to all connections. Each connection has its own count down, but the timeout value is global. When the interface has been idle for more than the configured period of time, the session will be terminated and will require authentication to establish a new session.

10.1 Setting the inactivity period

10.1.1 To set the inactivity period for both local CLI and remote SSH, use the following commands:

```
*A:SR-xx# configure system login-control idle-timeout <minutes>
```

11 Setting Login Banners

Security Administrators can create a customized pre-login message that will be displayed at the following interfaces:

- Local console CLI
- Remote SSH CLI

This banner will be displayed prior to allowing Security Administrator access through those interfaces.

11.1.1 Customizing Pre-login messages Using the local CLI and remote SSH Interfaces

Use the following command to configure the Login Banner:

```
*A:SR-xx# configure system login-control pre-login-message
<login-text-string>
```

***Note**: The message can be 900 characters long.*

12 References

- Nokia 7x50 SR OS 20.10.R12 for 7750 SR-7, 7750 SR-12, 7750 SR-12e, 7750 SR-1e, 7750 SR-2e, 7750 SR-3e, 7750 SR-a4, and 7750 SR-a8 with maxp10-10/1Gb-msec-sfp+ and me12-10/1gb-sfp+ MDAs Security Target v3.2

13 Acronym Table

Table 6 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
CA	Connectivity Association
CAK	Connectivity Association Key
CBC	Cipher Block Chaining
CKN	Connectivity Association Key Name
CLI	Command Line Interface
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DH	Diffie-Hellman
DNS	Domain Name System
FIPS	Federal Information Processing Standards
GCM	Galois Counter Mode
HMAC	Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPs	Hypertext Transfer Protocol Secure
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
MB	Megabyte
MKA	MACsec Key Agreement
NDcPP	Network Device collaborative Protection Profile
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
PP	Protection Profile
RAM	Random Access Memory
RFC	Requests for Comments
RSA	Rivest-Shamir-Adleman
SAK	Secure Association Key
SFR	Security Functional Requirement
SFP	Security Policy Database
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TLS	Transport Layer Security
TSF	TOE Security Functionality

Acronym	Definition
MDA	Media Dependent Adapter
MPLS	Multiprotocol Label Switching