

National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme



Validation Report

for the

Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR-2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e, Version 1.0

Report Number: CCEVS-VR-11183-2021

Dated: 10/21/21

Version: 1.0

**National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899**

**Department of Defense
ATTN: NIAP, Suite 6982
9800 Savage Road
Fort George G. Meade, MD 20755-6982**

ACKNOWLEDGEMENTS

Validation Team

Jim Donndelinger

Marybeth Pannock

Swapna Katikaneni

Aerospace Corporation

Common Criteria Testing Laboratory

Lead Evaluator: Dayanandini Pathmanathan

Tester: Minal Wankhede

Evaluator: Brad Mitchell

Acumen Security, LLC

Table of Contents

1	Executive Summary	5
2	Identification	7
3	Architectural Information	9
3.1.1	TOE Product Type	9
3.2	TOE Description.....	9
3.3	TOE Evaluated Configuration	14
3.4	Physical Scope of the TOE	14
4	Security Policy	15
4.1	Security Audit	15
4.2	Cryptographic Support	15
4.3	Identification and Authentication	18
4.4	Security Management	18
4.5	TOE Access	18
4.6	Protection of the TSF	18
4.7	Trusted Path/Channels	18
4.8	Excluded Functionality	18
5	Assumptions, Threats & Clarification of Scope	19
5.1	Assumptions	19
5.2	Threats.....	20
5.3	Organizational Security Policies	21
5.4	Clarification of Scope	22
6	Documentation	23
7	TOE Evaluated Configuration	24
7.1	Evaluated Configuration.....	24
7.2	Excluded Functionality	24
8	IT Product Testing	25
8.1	Developer Testing	25
8.2	Evaluation Team Independent Testing.....	25
9	Results of the Evaluation	26
9.1	Evaluation of Security Target	26
9.2	Evaluation of Development Documentation.....	26
9.3	Evaluation of Guidance Documents.....	27
9.4	Evaluation of Life Cycle Support Activities	27
9.5	Evaluation of Test Documentation and the Test Activity	27
9.6	Vulnerability Assessment Activity	27
9.7	Summary of Evaluation Results	28
10	Validator Comments & Recommendations	29
11	Annexes	30

12	Security Target	31
13	Glossary	32
14	Bibliography.....	33

1 Executive Summary

This Validation Report (VR) is intended to assist the end user of this product and any security certification Agent for that end user in determining the suitability of this Information Technology (IT) product for their environment. End users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this VR, which describes how those security claims were tested and evaluated and any restrictions on the evaluated configuration. Prospective users should carefully read the Assumptions and Clarification of Scope in Section 5 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e (TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and documented in the ST.

The evaluation was completed by Acumen Security in October 2021. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test report, all written by Acumen Security. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements defined in the U.S. Government Protection Profile for Security Requirements for collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].

The Target of Evaluation (TOE) identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev. 5) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev. 5), as interpreted by the Assurance Activities contained in the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e]. This Validation Report applies only to the specific version of the TOE as evaluated. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team provided guidance on technical issues and evaluation processes and reviewed the individual work units documented in the ETR and the Assurance Activities Report (AAR). The validation team found that the evaluation showed that the product satisfies all of the functional requirements and assurance requirements stated in the Security Target (ST). Based on these findings, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of

the testing laboratory in the evaluation technical report are consistent with the evidence produced.

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profiles containing Assurance Activities, which are interpretation of CEM work units specific to the technology described by the PP.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List.

Table 1 provides information needed to completely identify the product, including:

- The Target of Evaluation (TOE): the fully qualified identifier of the product as evaluated.
- The Security Target (ST), describing the security features, claims, and assurances of the product.
- The conformance result of the evaluation.
- The Protection Profile(s) to which the product is conformant.
- The organizations and individuals participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e [NDCPP v2.2e]
Security Target	Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Security Target
Evaluation Technical Report	Evaluation Technical Report for Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16, 7450 ESS, and 7750 SR-1e
CC Version	Version 3.1, Revision 5
Conformance Result	CC Part 2 Extended and CC Part 3 Conformant
Sponsor	Nokia Corporation
Developer	Nokia Corporation
Common Criteria Testing Lab (CCTL)	Acumen Security Rockville, MD
CCEVS Validators	Jim Donndelinger

	Marybeth Pannock Swapna Katikaneni
--	---------------------------------------

3 Architectural Information

The Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e (herein referred to as the TOE) is a network device with the high-performance, scale and flexibility to support a function for service provider, web scale and enterprise networks. The Nokia 7x50 routers utilize 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.

3.1.1 TOE Product Type

The TOE is a network device that is composed of hardware and software. It satisfies all of the criterion to meet the collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].




3.2 TOE Description




The TOE includes a wide range of physical platforms that share a mutual architecture and feature set. The 7750 series are chassis-based routers that provides a variety of high-speed interfaces (only Ethernet is within scope of this 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. The SR-1e does support MACsec functionality but the MACsec functionality is not in the scope of this evaluation.

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 successfully authenticate with the correct credentials.

The TOE is comprised of the following models:

Table 1 –TOE Physical Boundary Components

Platform Description	Processors
<p>7950 XRS-16c</p>  <p># of Cores: 10 Core Frequency: 1.5Ghz OS: Nokia SR OS Image Version: 20.10.R4 Part number: 3HE08121AA</p>	<p>Cavium OCTEON II CN6645</p>
<p>7450 ESS</p>  <p># of Cores: 10 Core Frequency: 1.5Ghz OS: Nokia SR OS Image Version: 20.10.R4 Part number: 3HE08432AA</p>	<p>Cavium OCTEON II CN6645</p>
<p>7750 SR-1</p>  <p># of Cores: 16 Core Frequency: 1.8Ghz OS: Nokia SR OS Image Version: 20.10.R4 Part Number: 3HE12298AA</p>	<p>Cavium OCTEON III CN7360</p>

Platform Description	Processors
<p>7750 SR-1s</p>  <p># of Cores: 16 Core Frequency: 1.8Ghz OS: Nokia SR OS Image Version: 20.10.R4 Part number: 3HE13809xx</p>	<p>Cavium OCTEON III CN7360</p>
<p>7750 SR-2s</p>  <p># of Cores: 16 Core Frequency: 1.8Ghz OS: Nokia SR OS Image Version: 20.10.R4 Part number: 3HE12379AA</p>	<p>Cavium OCTEON III CN7360</p>
<p>7750 SR-1e</p>  <p># of Cores: 10 Core Frequency: 1.3 Ghz OS: Nokia SR OS Image Version: 20.10.R4 Part number: 3HE10301AA</p>	<p>Cavium OCTEON II CN6645</p>

Platform Description	Processors
<p data-bbox="402 233 537 258">7750 SR -7s</p>  <p data-bbox="402 613 699 764"># of Cores: 10 Core Frequency: 1.5 Ghz OS: Nokia SR OS Image Version: 20.10.R4 Part number: 3HE10301AA</p>	<p data-bbox="824 485 1114 510">Cavium OCTEON II CN6645</p>
<p data-bbox="402 774 548 800">7750 SR -14s</p>  <p data-bbox="402 1239 699 1390"># of Cores: 10 Core Frequency: 1.5 Ghz OS: Nokia SR OS Image Version: 20.10.R4 Part number: 3HE10301AA</p>	<p data-bbox="824 1073 1114 1098">Cavium OCTEON II CN6645</p>


Platform Description	Processors
<p data-bbox="402 233 545 258">7950 XRS-20</p>  <p data-bbox="402 1031 802 1220"># of Cores: CPM: 20 cores, CPM2: 48 cores Frequency: CPM:1.5GHz, CPM2: 1.8GHz OS: Nokia SR OS Part number: 3HE07113AA</p>	<p data-bbox="824 730 1114 756">Cavium OCTEON II CN6645</p>

Figure 1 depicts the TOE boundary:

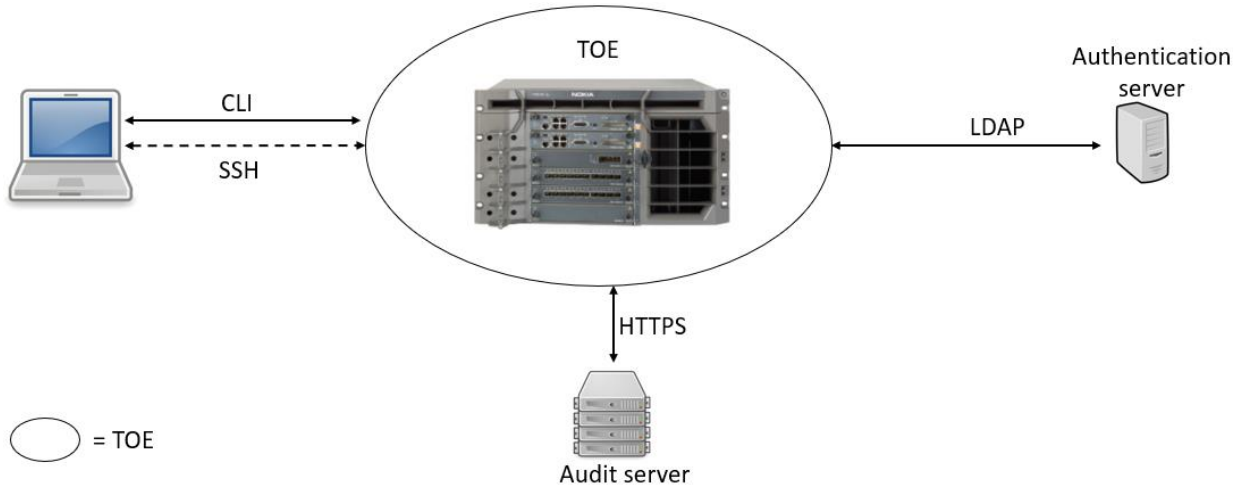


Figure 1 – TOE Boundary Diagram

3.3 TOE Evaluated Configuration

In the evaluated configuration, the TOE consists of one of the platforms identified above. The TOE supports secure connectivity with another IT environment device as stated in Table 3:

Table 2 – 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.
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.

3.4 Physical Scope of the TOE

The TOE boundary is the hardware appliance, which is comprised of hardware and software components. It is deployed in an environment that contains the various IT components as depicted in Figure 1 above. The TOE guidance documentation is included on the NIAP website.

4 Security Policy

The TOE implements the following security functional requirements:

- Security Audit
- Cryptographic Support
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channels

Each of these security functionalities are listed in more detail in the sections below.

4.1 Security Audit

The TOE generates audit events for all start-up and shut-down functions and all auditable events as specified in Table 15. Audit events are also generated for management actions specified in FAU_GEN.1. The TOE is capable of storing audit events locally and exporting them to an external audit server using HTTP PUT requests over TLS v1.2 protocol. Each audit record contains the date and time of event, type of event, subject identity, and the relevant data of the event. The audit server supports the following severity levels: indeterminate (info), major, and minor.

4.2 Cryptographic Support

The TOE provides cryptographic support for the services described in Table 4 below. The related CAVP validation details are provided in Table 5. The operating system is SR OS 20.10.R4. The TOE leverages OpenSSL v1.1.1g for its cryptographic functionality.

Table 3 – TOE Cryptography Implementation

Cryptographic Method	Usage
FCS_CKM.1 Cryptographic Key Generation	Cryptographic key generation conforming to FIPS PUB 186-4 Digital Signature Standard (DSS), Appendix B.3 and 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. RSA Key sizes supported are 2048 bits
FCS_CKM.2 Cryptographic Key Establishment	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 FFC Schemes using "safe-prime" groups that meet the following: 'NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [groups listed in RFC 3526].
FCS_CKM.4 Cryptographic Key Destruction	Refer to [ST] Table 19 for Key Zeroization details.
FCS_COP.1/DataEncryption	AES encryption and decryption conforming to CBC as specified in ISO 10116, CTR as specified in ISO 10116 and GCM as specified in ISO 19772. AES key size supported is 128 bits and 256 bits AES modes supported are: CBC, CTR and GCM.

Cryptographic Method	Usage
FCS_COP.1/SigGen	RSA digital signature algorithm conforming to 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. RSA key size of 2048 bits.
FCS_COP.1/Hash	Cryptographic hashing services conforming to ISO/IEC 10118-3:2004. Hashing algorithms supported are SHA-1, SHA-256, SHA-384, and SHA-512. Message digest sizes supported are: 160, 256, 384 and 512 bits.
FCS_COP.1/KeyedHash	Keyed-hash message authentication conforming to ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2". Keyed-hash algorithm supported are HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384 and HMAC-SHA-512. Key sizes supported are: 160, 256, 384, and 512 bits. Message digest sizes supported are: 160, 256, 384 and 512 bits.
FCS_RBG_EXT.1 Random Bit Generation	Random number generation conforming to ISO/IEC 18031:2011. The TOE leverages CTR_DRBG(AES) CTR_DRBG seeded with a minimum of 256 bits of entropy.
FCS_HTTPS_EXT.1 HTTPS Protocol	The TOE supports HTTPS protocol that complies with RFC 2818. The TOE implements HTTPS protocol using TLS v1.2 in support of the audit server.
FCS_TLSC_EXT.1 TLS Client Protocol	The TOE supports TLS v1.2 protocol for use with X. 509v3 based authentication. The following ciphersuites in the evaluated configuration: TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 3268 TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 3268 TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246 TLS_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 5246
FCS_SSHS_EXT.1 SSH Client Protocol	The TOE supports SSH v2 protocol compliant to the following RFCs: 4251, 4252, 4253, 4254, 4344, 5647, 8268, 6668. The TOE supports public key and password-based authentication. SSH public-key authentication uses ssh-rsa. SSH transport uses the following encryption algorithms: aes128-ctr, aes128-cbc, aes256-cbc and aes256-ctr. Packets greater than 256K bytes in an SSH transport connection are dropped. SSH transport uses the following data integrity MAC algorithms: hmac-sha1, hmac-sha256, and hmac-sha2-512. Key exchange algorithms supported are diffie-hellman-group14-sha256, diffie-hellman-group14-sha1 and diffie-hellman-group16-sha512. The TOE ensures that within SSH connections the same session keys are used for a threshold of no longer than one hour and no more than one gigabyte of transmitted data.

The related CAVP validation details are provided in Table 5. The operating system is SR OS 20.10.R1. The TOE leverages the OpenSSL v 1.1.1g for its cryptographic functionality.

Table 4 – CAVP Algorithm Testing References

Cryptographic Algorithms	CAVPS	Implementation Library	Operational Environment (OE)
AES	C2074	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON III CN7360
	C2075	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON II CN6645
RSA	C2074	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON III CN7360
	C2075	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON II CN6645
HMAC	C2074	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON III CN7360
	C2075	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON II CN6645
SHS	C2074	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON III CN7360
	C2075	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON II CN6645
DRBG	C2074	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON III CN7360
	C2075	Nokia 7x50 SR OS Cryptographic Library	Cavium OCTEON II CN6645

Keys/CSPs	Purpose	Storage Location	Method of Zeroization
Diffie-Hellman Shared Secret	The shared secret used in Diffie-Hellman (DH) exchange. Created per the Diffie-Hellman Exchange.	RAM	A single overwrite consisting of zeroes.
Diffie Hellman private key	The private key used in Diffie-Hellman (DH) Exchange	RAM	A single overwrite consisting of zeroes.
SSH Private key	The SSH server host private key is stored on the local filesystem	RAM; CF if preserve-key is enabled.	A single overwrite consisting of zeroes.
SSH Session Key	These are the session keys for SSH.	RAM	A single overwrite consisting of zeroes.
TLS Session Keys	These are the session keys for TLS.	RAM	A single overwrite consisting of zeroes.
RNG Seed Key	This is the seed key for the RNG.	RAM	A single overwrite consisting of zeroes.
RNG Seed	This seed is for the RNG.	RAM	A single overwrite consisting of zeroes

4.3 Identification and Authentication

All users must be authenticated to the TOE prior to carrying out any management actions. The TOE supports password-based authentication and public key-based authentication. Based on the assigned role, a user is granted a set of privileges to access the system.

4.4 Security Management

The TOE supports local and remote management of its security functions including:

- Local console CLI administration
- Remote CLI administration via SSHv2
- Timed user lockout after multiple failed authentication attempts
- Password configurations
- Configurable banners to be displayed at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Protection of secret keys and passwords

4.5 TOE Access

Prior to establishing an administration session with the TOE, a banner is displayed to the user. The banner messaging is customizable. The TOE will terminate an interactive session after configurable number of minutes of session inactivity. A user can terminate their local CLI session and remote CLI session by entering the appropriate command at the prompt.

4.6 Protection of the TSF

The TOE protects all passwords, pre-shared keys, symmetric keys, and private keys from unauthorized disclosure. Pre-shared keys, symmetric keys, and private keys are stored in encrypted format. Passwords are stored as a non-reversible hash value as per standard Linux approach. The TOE executes self-tests during initial start-up to ensure correct operation and enforcement of its security functions. An administrator can install software updates to the TOE. The TOE internally maintains the date and time.

4.7 Trusted Path/Channels

The TOE supports HTTPS PUT requests over TLS v1.2 for secure communication to the audit server. The TOE supports TLS v1.2 for secure communication to LDAP server. The TOE supports local CLI and uses SSH v2 for secure remote administration.

4.8 Excluded Functionality

The following interfaces are not included as part of the evaluated configuration:

- gRPC is disabled
- telnet is disabled
- MACsec functionality is not evaluated
- SNMP is not evaluated

5 Assumptions, Threats & Clarification of Scope

5.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

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).
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).
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

ID	Assumption
	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.

5.2 Threats

The following table lists the threats addressed by the TOE and the IT Environment. The assumed level of expertise of the attacker for all the threats identified below is Enhanced-Basic.

ID	Threat
T.UNAUTHORIZED_ADMINISTRATOR_ACCESS	Threat agents may attempt to gain Administrator access to the network device by nefarious means such as masquerading as an Administrator to the device, masquerading as the device to an Administrator, replaying an administrative session (in its entirety, or selected portions), or performing man-in-the-middle attacks, which would provide access to the administrative session, or sessions between network devices. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target network devices that do not use standardized secure tunneling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols or poor key management to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network

ID	Threat
	traffic, and potentially could lead to a compromise of the network device itself.
T.WEAK_AUTHENTICATION_ENDPOINTS	Threat agents may take advantage of secure protocols that use weak methods to authenticate the endpoints, e.g., a shared password that is guessable or transported as plaintext. The consequences are the same as a poorly designed protocol, the attacker could masquerade as the Administrator or another device, and the attacker could insert themselves into the network stream and perform a man-in-the-middle attack. The result is the critical network traffic is exposed and there could be a loss of confidentiality and integrity, and potentially the Network Device itself could be compromised.
T.UPDATE_COMPROMISE	Threat agents may attempt to provide a compromised update of the software or firmware which undermines the security functionality of the device. Non-validated updates or updates validated using non-secure or weak cryptography leave the update firmware vulnerable to surreptitious alteration.
T.UNDETECTED_ACTIVITY	Threat agents may attempt to access, change, and/or modify the security functionality of the network device without Administrator awareness. This could result in the attacker finding an avenue (e.g., misconfiguration, flaw in the product) to compromise the device and the Administrator would have no knowledge that the device has been compromised.
T.SECURITY_FUNCTIONALITY_COMPROMISE	Threat agents may compromise credentials and device data enabling continued access to the network device and its critical data. The compromise of credentials includes replacing existing credentials with an attacker's credentials, modifying existing credentials, or obtaining the Administrator or device credentials for use by the attacker.
T.PASSWORD_CRACKING	Threat agents may be able to take advantage of weak administrative passwords to gain privileged access to the device. Having privileged access to the device provides the attacker unfettered access to the network traffic and may allow them to take advantage of any trust relationships with other Network Devices.
T.SECURITY_FUNCTIONALITY_FAILURE	An external, unauthorized entity could make use of failed or compromised security functionality and might therefore subsequently use or abuse security functions without prior authentication to access, change or modify device data, critical network traffic or security functionality of the device.

5.3 Organizational Security Policies

The OSPs included in Table 11 are drawn directly from the [NDcPP v2.2e]

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

5.4 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance. The level of assurance for this evaluation is defined within the Collaborative Protection Profile for Network Devices, Version 2.2e [NDcPP v2.2e].
- Consistent with the expectations of the Protection Profile, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.
- The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs. Any additional security related functional capabilities included in the product were not covered by this evaluation.
- This evaluation covers only the specific device models and software as identified in this document, and not any earlier or later versions released or in process
- Consumers employing the TOE must follow the configuration instructions provided in the CC Configuration Guidance documentation listed in Section 6 to ensure the evaluated configuration is established and maintained.
- Consumers need to pay specific attention to all the functionality and features that are explicitly excluded from the scope of the evaluation and are identified in section 7.2

6 Documentation

The following documents were provided by the vendor with the TOE for evaluation:

[ST]	Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Security Target	3.0	October 12, 2021
[AGD]	Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Guidance Document	0.7	October 12, 2021

These are the only documents that should be trusted for the configuration, administration, and use of the TOE in the evaluated configuration. If other documents are referenced in CC Configuration Guide, only the sections of other documents referenced should be trusted and used to configure and operate the TOE.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the TOE as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated configuration of the TOE is described in section 3 of this document.

7.2 Excluded Functionality

The following interfaces are not included as part of the evaluated configuration:

- NTP server
- gRPC is disabled
- telnet is disabled
- MACsec functionality is not evaluated
- SNMP is not evaluated
- MPLS is not evaluated

8 IT Product Testing

This section describes the testing efforts of the developer and the evaluation team. It is derived from information contained in Evaluation Test Report for Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e, which is not publicly available. The Assurance Activities Report[AAR] provides an overview of testing and the prescribed assurance activities.

8.1 Developer Testing

No evidence of developer testing is required in the Assurance Activities for this product.

8.2 Evaluation Team Independent Testing

The evaluation team verified the product according the vendor-provided guidance documentation and ran the tests specified in the [NDcPP v2.2e]. The Independent Testing activity is documented in the Assurance Activities Report, which is publicly available, and is not duplicated here.

9 Results of the Evaluation

The results of the assurance requirements are generally described in this section and are presented in detail in the proprietary documents: the Detailed Test Report (DTR) and the Evaluation Technical Report (ETR). The reader of this document can assume that activities and work units received a passing verdict.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1 rev 4 and CEM version 3.1 rev 4. The evaluation determined the Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e to be Part 2 extended, and meets the SARs contained in the PP. Additionally the evaluator performed the Assurance Activities specified in the NDPP.

9.1 Evaluation of Security Target

The evaluation team applied each ASE CEM work unit. The ST evaluation ensured the ST contains a description of the environment in terms of policies and assumptions, a statement of security requirements claimed to be met by the Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e that are consistent with the Common Criteria, and product security function descriptions that support the requirements. Additionally, the evaluator performed an assessment of the Assurance Activities specified in the [NDcPP v2.2e].

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of Development Documentation

The evaluation team applied each EAL 1 ADV CEM work unit. The evaluation team assessed the design documentation and found it adequate to aid in understanding how the TSF provides the security functions. The design documentation consists of a functional specification contained in the Security Target's TOE Summary Specification. Additionally, the evaluator performed the Assurance Activities specified in the [NDcPP v2.2e] related to the examination of the information contained in the TOE Summary Specification.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of Guidance Documents

The evaluation team applied each EAL 1 AGD CEM work unit. The evaluation team ensured the adequacy of the user guidance in describing how to use the operational TOE. Additionally, the evaluation team ensured the adequacy of the administrator guidance in describing how to securely administer the TOE. The guides were assessed during the design and testing phases of the evaluation to ensure they were complete. Additionally, the evaluator performed the Assurance Activities specified in the [NDcPP v2.2e] related to the examination of the information contained in the operational guidance documents.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the Assurance Activities, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of Life Cycle Support Activities

The evaluation team applied each EAL 1 ALC CEM work unit. The evaluation team found that the TOE was identified.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of Test Documentation and the Test Activity

The evaluation team applied each EAL 1 ATE CEM work unit. The evaluation team ran the set of tests specified by the Assurance Activities in the [NDcPP v2.2e] and recorded the results in a Test Report, summarized in the Evaluation Technical Report and Assurance Activities Report.

The validator reviewed the work of the evaluation team and found that sufficient evidence was provided by the evaluation team to show that the evaluation activities addressed the test activities in the [NDcPP v2.2e], and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity

The evaluation team applied each EAL 1 AVA CEM work unit. The evaluation team performed a public search for vulnerabilities, performed vulnerability testing and did not discover any issues with the TOE.

The validator reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation addressed the vulnerability analysis Assurance Activities in the [NDcPP v2.2e], and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team's assessment of the evaluation evidence demonstrates that the claims in the ST are met. Additionally, the evaluation team's test activities also demonstrated the accuracy of the claims in the ST.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the Assurance Activities in the [NDcPP 2.2e], and correctly verified that the product meets the claims in the ST.

10 Validator Comments & Recommendations

The validation team notes that the evaluated configuration is dependent upon the TOE being configured per the evaluated configuration instructions in the Configuration for Common Criteria Guide. The excluded functionality is specified in section 7.2 of this report. All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

[ST]	Nokia 7x50 SR OS 20.10.R4 for 7750 SR-1, 7750 SR-1s, 7750 SR- 2s, 7750 SR-7s, 7750 SR-14s, 7950 XRS-20, 7950 XRS-16c, 7450 ESS, and 7750 SR-1e Security Target	3.0	October 12, 2021
------	--	-----	------------------

13 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL).** An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance.** The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation.** The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology to determine whether or not the claims made are justified; or the assessment of a protection profile against the Common Criteria using the Common Evaluation Methodology to determine if the Profile is complete, consistent, technically sound and hence suitable for use as a statement of requirements for one or more TOEs that may be evaluated.
- **Evaluation Evidence.** Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE).** A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation.** The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body.** A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

1. Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model, Version 3.1 Revision 5.
2. Common Criteria for Information Technology Security Evaluation - Part 2: Security functional requirements, Version 3.1 Revision 5.
3. Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance requirements, Version 3.1 Revision 5.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5.