National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for the

Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms

Report Number: CCEVS-VR-VD11615-2025
Dated: 9 September 2025
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

Jenn Dotson

Lisa Mitchell

Clare Parran

Lori Sarem

The MITRE Corporation

Common Criteria Testing Laboratory

Theo Ajibade

Rupal Gupta

Akshay Jain

Acumen Security, LLC

Table of Contents

1 Executive Summary

This report documents the National Information Assurance Partnership (NIAP) Validation team's assessment of the evaluation of the Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms. It presents the evaluation results, their justifications, and the conformance results. This Validation Report (VR) is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

The evaluation was performed by the Acumen Security Common Criteria Testing Laboratory (CCTL) in Rockville, Maryland, USA, and was completed in September 2025. The information in this report is largely derived from the Evaluation Technical Report (ETR) and associated test reports, 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 of the:

- *PP-Configuration for Network Devices and MACsec Ethernet Encryption*, 2023-03-29

  This PP-Configuration includes the following:

  - Base-PP: *collaborative Protection Profile for Network Devices*, Version 3.0e [CPP_ND_V3.0E]
  - PP-Module: *PP-Module for MACsec Ethernet Encryption*, Version 1.0 [MOD_MACsec_V1.0]

- *Functional Package for SSH Version 1.0* [PKG_SSH_V1.0]

The TOE is the Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms. The TOE identified in this VR has been evaluated at a NIAP approved CCTL 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). This VR 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 (CCEVS) and the conclusions of the testing laboratory in the ETR are consistent with the evidence provided.

The Validation team monitored the activities of the Evaluation team, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and successive versions of the ETR. The Validation team found that the evaluation showed that the product satisfies all the functional requirements and assurance requirements stated in the Security Target (ST). Therefore, 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 ETR are consistent with the evidence produced.

The technical information included in this report was obtained from the *Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Security Target*, Version 1.2, August 22, 2025, and analysis performed by the Validation team.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of IT 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 Validated Products 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 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms
Protection Profile	*PP-Configuration for Network Devices and MACsec Ethernet Encryption*, 2023-03-29 This PP-Configuration includes the following: • Base-PP: *collaborative Protection Profile for Network Devices*, Version 3.0e [CPP_ND_V3.0E] • PP-Module: *PP-Module for MACsec Ethernet Encryption*, Version 1.0 [MOD_MACsec_V1.0] *Functional Package for SSH Version 1.0* [PKG_SSH_V1.0]
Security Target	*Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Security Target*, Version 1.2, August 22, 2025
Evaluation Technical Report	*Evaluation Technical Report for Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms*, Version 0.6, August 25, 2025
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	Jenn Dotson, Lisa Mitchell, Clare Parran, Lori Sarem

3 Architectural Information

3.1 TOE Description

The Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms (herein referred to as the TOE) are a network devices that utilizes Nokia's SR operating system version 24.10.R3. The Nokia 7750 Service Router (SR) & 7250 Interconnect Router (IXR) portfolios include 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. The Nokia 7750 SR & 7250 IXR portfolios are chassis-based routers.

The Nokia 7750 SR portfolio consists of hardware platforms intended for use in IP edge and core networking environments. The portfolio includes the 7750 SR-s and 7750 SR series appliance families. The following Table 2 lists the specifically evaluated Nokia platforms:

Table 2 – Nokia 7750 SR Platforms

Platforms (part number)	CPU	Speed	Core
7750 SR-1 CPM in: -7750 SR-1 (FP4)	Marvell OCTEON III CN7360 (MIPS64)	1.8GHz	16
7750 SR-1 CPM in: -7750 SR-1-24D -7750 SR-1-48D -7750 SR-1-46S -7750 SR-1-92S	AMD EPYC3251 (ZEN)	2.5GHz	8
7750 SR-1x in: -7750 SR-1x-48D -7750 SR-1x-92S	AMD EPYC3251 (ZEN)	2.5GHz	8
7750 SR-1se CPM	AMD EPYC3251 (ZEN)	2.5GHz	8
7750 SR-2se CPM-2se	AMD EPYC3251 (ZEN)	2.5GHz	8
7750 SR-2s CPM	Marvell OCTEON III CN7360 (MIPS64)	1.8GHz	16
7750 SR-14s/7s CPM-s v2	Marvell OCTEON III CN7890 (MIPS64)	1.8GHz	48
7750 SR-7/SR-12/SR-12e SR CPM5	Marvell OCTEON II CN6645 (MIPS64)	1.5GHz	10

The Nokia 7250 IXR portfolio includes the following appliance families: The 7250 IXR-R, IXR-e, IXR-X and 7250 IXR-s platforms. The following Table 3 lists the specifically evaluated Nokia 7250 IXR platforms:

Table 3 - Nokia 7250 IXR Platforms

Platforms (part number)	CPU	Speed	Core
7250 IXR-R6d/dl CPIOM	AMD EPYC3255 (ZEN)	2.5GHz	8
7250 IXR-e (Small) CPM	Intel Atom C3708 (Goldmont)	1.7GHz	8
7250 IXR-R4 CPM	Marvell OCTEON III CN7340 (MIPS64)	1.5GHz	8
7250 IXR-R6 CPIOM	Marvell OCTEON III CN7360	1.5GHz	16

The TOE supports a full array of network functions and services. 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 this evaluation) for various scales of networks and various network applications. The TOE utilizes a common Nokia SR operating system, features, and technology for compatibility across all platforms.

Nokia SR OS 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). On the evaluated configuration, the TOE permits only EAPOL (PAE EtherType 88-8E), MACsec frames (EtherType 88-E5), and MAC control frames (EtherType 88-08) and discards others.

The TOE provides AES-GCM MACsec encryption. The MACsec feature is powered by one or more of the network processor chips listed in Table 4:

Table 4 – TOE's MACsec PHYs

Network Chip	Vendor
BCM82399	Broadcom
BCM81392	
BCM81394	
BCM81343	
VSC8258	Microsemi
VSC8490	
VSC8584	
E5	Nokia

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 Table 5 lists the TOE platforms and their compatible MDA card, in addition to the MACsec PHY:

Table 5 – MDA and MACsec cards used in the TOE's MACsec capable appliances

TOE platforms	MACsec card	MACsec embedded (network processor) PHY (ethernet PHY framer)
7750 SR-1se CPM	ms36-800g-qsfpdd	Nokia E5
7750 SR-1-48D CPM	m48-400g-qsfpdd-1	
7750 SR-1x-92S CPM	m80-200g-sfpdd+12-800g-qsfpdd-1x	

TOE platforms	MACsec card	MACsec embedded (network processor) PHY (ethernet PHY framer)
7750 SR-1-92S CPM	m80-200g-sfpdd+12-400g-qsfpdd-1	
7750 SR-1-24D CPM	m24-800g-qsfpdd-1	
7750 SR-1x-48D CPM	m48-800g-qsfpdd-1x	
7750 SR-1-46S CPM	m40-200g-sfpdd+6-800g-qsfpdd-1	
7750 SR-2se CPM	x2-s36-800g-qsfpdd-18.0t	Nokia E5
	x2-s18-800g-qsfpdd	
	x2-s36-800g-qsfpdd-12.0t	
	mse24-200g-sfpdd	
	mse6-800g-cfp2-dco	
	mse14-800g+4-400g	
	m36-800g-qsfpdd	
	mse6-800g-qsfpdd	
	m36-400g-qsfp112	
7250 IXR-R6d/R6dl CPIOM	m20-10g-sfp+	VSC8258
	m18-25g-sfp28	BCM81392 and BCM81394
	m1-400g-qsfpdd+1-100g-qsfp28	BCM81343
	m46-10g-sfp+	VSC8258
	m2-cfp2	BCM81343
	m32-1g-csfp	VSC8584
	m80-1g-csfp	VSC8584
	m2-100g-qsfp28+16-10g-sfp+	BCM81392 and VSC8258
7750 SR-14s/7s CPM-s v2 (SR-s CPM-2S)	x2-s36-800g-qsfpdd-18.0t	Nokia E5
	x2-s18-800g-qsfpdd	
	x2-s36-800g-qsfpdd-12.0t	
	ms16-sdd+4-qsfp28-b	BCM81343
	ms8-sdd+2-qsfp28-b	BCM81343
	mse24-200g-sfpdd	Nokia E5
	mse6-800g-cfp2-dco	

TOE platforms	MACsec card	MACsec embedded (network processor) PHY (ethernet PHY framer)
	mse14-800g+4-400g	
	m36-800g-qsfpdd	
	mse6-800g-qsfpdd	
	m36-400g-qsfp112	
7750 SR-2s CPM	ms16-sdd+4-qsfp28-b	BCM81343
	ms8-sdd+2-qsfp28-b	BCM81343
7750 SR-7 & SR-12 & SR-12e SR CPM5	me16-25gb-sfp28+2-100gb-qsfp-b	BCM81343
7750 SR-1 CPM	me16-25gb-sfp28+2-100gb-qsfp-b	BCM81343
7250 IXR-R6 CPIOM	m10-10g-sfp+	VSC8258
	m20-1g-csfp	VSC8584
	m6-10g-sfp++1-100g-qsfp28	BCM82399 and VSC8258
	m4-10g-sfp++1-100g-cfp2	BCM82399 and VSC8258
	m6-10g-sfp++4-25g-sfp28	BCM82399 and VSC8258
7250 IXR-R4 CPM	m10-10g-sfp+	VSC8258
	m20-1g-csfp	VSC8584
	m6-10g-sfp++1-100g-qsfp28	BCM82399 and VSC8258
	m4-10g-sfp++1-100g-cfp2	BCM82399 and VSC8258
	m6-10g-sfp++4-25g-sfp28	BCM82399 and VSC8258
7250 IXR-e CPM (small)	m14-10g-sfp++4-1g-tx	VSC8490

Some TOE models, such as the 7250 IXR-R4 and 7250 IXR-R6, can be equipped with an MDA that includes two types of MACsec PHYs. These MDAs use both PHYs to handle MACsec protocols, resulting in certain ports on the MDA card using different PHYs for MACsec traffic encryption.

The MACsec Key Agreement (MKA) protocol uses the Connectivity Association Key (CAK) to derive a Key Encryption Key (KEK), which secures the distribution of transient session keys called Secure Association Keys (SAKs). SAKs and other MKA parameters are required to sustain communication over 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
- Multipoint-to-multipoint mode

In the evaluated configuration, MACsec is configured individually on a point-to-point Ethernet link. A pair of MACsec devices can be connected via bridge or a direct connection. To enable secure MACsec communication, devices use the pre-shared Connectivity Association Key (CAK) to authenticate each other and execute the MACsec Key Agreement (MKA) protocol. MKA negotiates and distributes transient Secure Association Keys (SAKs), which are then used to encrypt/decrypt data traffic over the MACsec-secured channel.

In order to determine an authorized peer, both devices must first exchange an MKA frame, and these devices must agree upon a shared key and MACsec cipher suite in order to set up both receive and transmit Security Associations (SA). Once the connections are established, the MACsec frames will be transmitted between devices. **Error! Reference source not found.** depicts the TOE boundary.

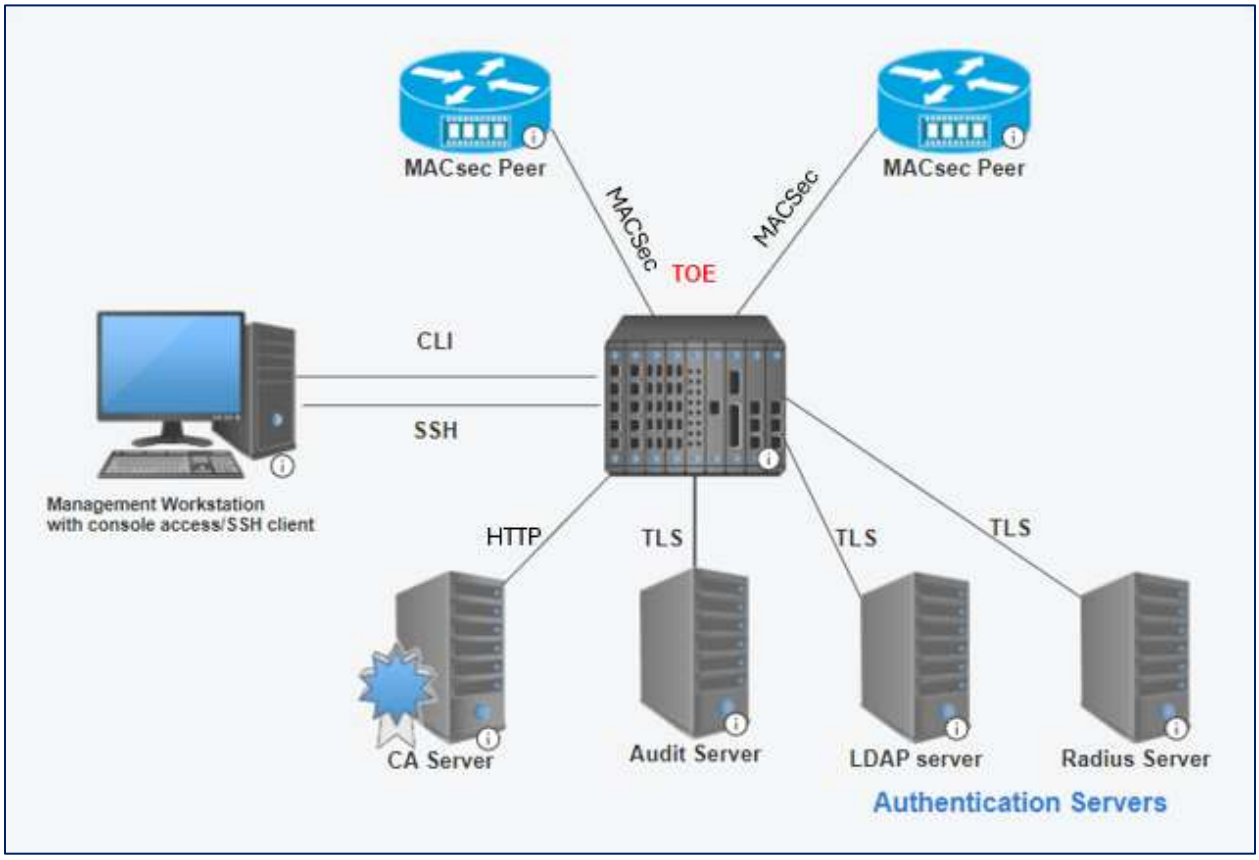

Figure 1 – TOE Boundary Diagram

3.2 TOE Evaluated Configuration

In the evaluated configuration, the TOE consists of the platforms as stated in Section 3.1. The TOE supports secure connectivity with other IT environment devices as stated in Table 6.

Table 6– IT Environment Components

Components	Required (Y/N)	Protocols used	Usage
Audit server	Yes	TLS	The audit server supports Syslog over TLS v1.2 to receive audit events securely from the TOE.

Components	Required (Y/N)	Protocols used	Usage
LDAP server	Yes	TLS	This server will provide the authentication mechanism to authenticate users.
RADIUS Server	Yes	TLS	This server will provide the authentication mechanism to authenticate users.
MACsec peer	Yes	MACsec	This peer is required to test MACsec functionality.
Management workstation with console access/SSH client	Yes	CLI-SSH	This includes any IT Environment Management workstation with console access and an SSH client.
Certificate Authority server	Yes	HTTP	The Certificate Authority server is used for issuing, generation and management of X509 certificates to be used with the TOE.

3.3 Physical Scope of the TOE

The TOE boundary is the hardware appliance, which is comprised of hardware and software components. The software component is SROS v24.10.R3 running on TiMOS SMP v2.5 and using the SR Crypto Module (SRCM) version 5.0. It is deployed in an environment that contains the various IT components as depicted in Figure 1 above. SROS version 24.10.R3 is a software that includes various router applications, the SR Cryptographic Module (SRCM) and the TiMOS SMP Kernel. The TiMOS SMP Kernel serves as the main interface between the router's physical hardware and the router's applications running on it. The kernel enables multiple applications to share hardware resources by providing access to CPU, memory, mass storage and networking.

4 Security Policy

4.1 Logical Scope of the TOE

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.

4.1.1 Security Audit

The TOE generates audit events for all start-up and shut-down functions and all auditable events as specified in Table 20 of the ST. 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 Syslog protocol over TLS v1.2 protocol. The TOE uses the Syslog protocol over TLS to transmit audit events in real-time, as they are generated, to an external audit server. Each audit record includes the date and time of the event, the event type, the identity of the subject, and any relevant event data.

4.1.2 Cryptographic Support

The TOE provides cryptographic support for the services described in the tables below. The related CAVP validation details are provided in Table 7. The operating system is SROS version 24.10.R3 running on TiMOS SMP version 2.5. The TOE leverages Nokia SR Cryptographic Module (SRCM) version 5 which is based on OpenSSL v3.1 library and incorporates the FIPS module 3.1.6-nokia.1.0 as its FIPS provider, to provide its cryptographic functionality.

Table 7: TOE's CAVP Algorithm references

SFRs	Algorithm in ST	Implementation Name	CAVP Alg	CAVP Cert
FCS_CKM.1	RSA schemes using cryptographic key sizes of [2048, 3072 and 4096 bits] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", A.1.	Nokia SR Cryptographic Module (SRCM) version 5.0	RSA KeyGen (FIPS186-5)	A5455
	ECC schemes using 'NIST curves' [P-256, P-384, P-521] that meet the following: FIPS PUB 186-4,		ECDSA KeyGen (FIPS186-5)	A5455

	"Digital Signature Standard (DSS)", Appendix B.4, or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Appendix A.2, or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.		ECDSA KeyVer (FIPS186-5)	
	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]		Lab tested using known good implementation	No NIST CAVP, CCTL has performed all assurance/evaluation activities and documented in the ETR and AAR accordingly.
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.2"	Nokia SR Cryptographic Module (SRCM) version 5.0	Lab tested using known good implementation	No NIST CAVP, CCTL has performed all assurance/evaluation activities and documented in the ETR and AAR accordingly.
	Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 3, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"		KAS-ECC-SSC Sp800-56Ar3	A5455
	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]		Lab tested using known good implementation	No NIST CAVP, CCTL has performed all assurance/evaluation activities and documented in the ETR and AAR accordingly.
FCS_COP.1/ DataEncryption	GCM mode and cryptographic key sizes 128 bits, 256 bits that meet: AES as specified in ISO 18033-3 and GCM as specified in ISO 19772	Nokia SR Cryptographic Module (SRCM) version 5.0	AES-GCM	A5455

	CBC mode and cryptographic key sizes 128 bits, 256 bits that meet: AES as specified in ISO 18033-3, CBC as specified in ISO 10116.		AES-CBC	
	CTR mode and cryptographic key sizes 128 bits, 256 bits that meet: AES as specified in ISO 18033-3, and CTR as specified in ISO 10116.		AES-CTR	
FCS_COP.1/ SigGen	RSA Digital Signature Algorithm using key sizes of 2048, 3072 and 4096 bits that meets FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 5.4 using PKCS #1 v2.2 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Nokia SR Cryptographic Module (SRCM) version 5.0	RSA SigGen (FIPS186-5) RSA SigVer (FIPS186-5)	A5455
	ECDSA schemes implementing [P-256, P-384, P-521] curves that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 6 and Appendix D, Implementing “NIST Recommended" curves ; or FIPS PUB 186-5, "Digital Signature Standard (DSS)", Section 6 and NIST SP 800-186 Section 3.2.1, Implementing Weierstrass curves; or ISO/IEC 14888-3, "IT Security techniques - Digital signatures with appendix - Part 3: Discrete logarithm based mechanisms", Section 6.6.		ECDSA SigGen (FIPS186-5) ECDSA SigVer (FIPS186-5)	
FCS_COP.1/ Hash	SHA-1, SHA-256, SHA-384 and SHA-512 and message digest sizes 160, 256, 384 and 512 bits	Nokia SR Cryptographic Module (SRCM) version 5.0	SHA-1 SHA2-256 SHA2-384 SHA2-512	A5455

FCS_COP.1/ KeyedHash	HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512 with key sizes 160 bits, 256 bits, 384 bits, 512 bits and message digest 160, 256, 384, 512 bits that meet the following: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"	Nokia SR Cryptographic Module (SRCM) version 5.0	HMAC-SHA-1 HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512	A5455
FCS_COP.1/ CMAC	keyed-hash message authentication with AES-CMAC and key sizes 128, 256 bits and message digest size of 128 bits that meets: NIST SP 800-38B.	Nokia SR Cryptographic Module (SRCM) version 5.0	AES-CMAC	A5455
FCS_COP.1/ MACSEC	Encryption and decryption in accordance with AES used in AES Key Wrap and key sizes 128 , 256 bits that meets AES as specified in ISO 18033-3, AES Key Wrap as specified in NIST SP 800-38F. Encryption and decryption in accordance with GCM and key sizes 128 , 256 bits that meets AES as specified in ISO 18033-3, GCM as specified in ISO 19772.	Nokia SR Cryptographic Module (SRCM) version 5.0	AES-KW AES-GCM	A5455
FCS_RBG_EXT.1	CTR_DRBG (AES) in accordance with ISO/IEC 18031:2011 with a minimum of 256-bits	Nokia SR Cryptographic Module (SRCM) version 5.0	Counter DRBG	A5455

The Broadcom PHY BCM81394 integrates two BCM81392 dies. As a result, each BCM81392 supports half the data rate per channel on the system side and half the number of 100G/10G ports. Additionally, PHY chips from Broadcom, Microsemi (now part of Microchip), and Nokia's E5 series are used to perform AES-GCM encryption and decryption for the MACsec protocol. These PHYs have undergone CAVP testing by NIST to validate their cryptographic compliance.

Table 8: MACsec PHYs CAVP Algorithm Testing References

Cryptographic Algorithms	CAVPS	Implementation Library	PHY devices	Operational Environment (OE)
AES-GCM	AES 3969	Microsemi Intellisec 10G PHY	VSC8258	Microsemi Intellisec 10G PHY
	AES 3191	Vitesse Intellisec 10G PHY	VSC8258	Vitesse Intellisec 10G PHY
	AES 3504	Microsemi Intellisec 1G PHY	VSC85xx	Microsemi Intellisec 1G PHY

Cryptographic Algorithms	CAVPS	Implementation Library	PHY devices	Operational Environment (OE)
	AES 2781	Vitesse Intellisec 10G PHY	VSC8490/91	Mentor Graphics Questasim 10.0d
	AES 4545	AES ECB 128bit & 256bit Encryption/Decryption Engine	BCM82396, BCM59202, BCM82399	AES ECB 128bit & 256bit Encryption/Decryption Engine
	C1877	AES ECB 128bit & 256bit Encryption/Decryption Engine	BCM81343, BCM81392, BCM81394, BCM81398	AES ECB 128bit & 256bit Encryption/Decryption Engine
	A5786	400G MACsec Encryption/Decryption Engine on Nokia E5	Nokia E5	Synopsys VCS 2023.03-SP2

4.1.3 Identification and Authentication

The TOE supports Role Based Access Control. 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.

4.1.4 Security Management

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

- Ability to administer the TOE remotely
- Ability to configure the access banner
- Ability to configure the remote session inactivity time before session termination
- Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates
- Ability to configure local audit behaviour (e.g. changes to storage locations for audit; changes to behaviour when local audit storage space is full; changes to local audit storage size)
- Ability to modify the behaviour of the transmission of audit data to an external IT entity
- Ability to configure the cryptographic functionality
- Ability to configure thresholds for SSH rekeying
- Ability to set the time which is used for time-stamps
- Ability to manage the cryptographic keys
- Ability to manage the TOE's trust store and designate X509.v3 certificates as trust anchors
- Ability to generate Certificate Signing Request (CSR) and process CA certificate response
- Ability to administer the TOE locally
- Ability to configure the local session inactivity time before session termination or locking
- Ability to configure the authentication failure parameters for FIA_AFL.1
- Ability to manage the trusted public keys database
- Ability to configure the list of supported (D)TLS ciphers;

- Manage a PSK-based CAK and install it in the device
- Manage the key server to create, delete, and activate MKA participants [as specified in IEEE 802.1X-2020, Sections 9.13 and 9.16 (cf. MIB object ieee8021XKayMkaParticipant Entry) and section 12.2 (cf. function createMKA()]
- Specify the lifetime of a CAK
- Enable, disable, or delete a PSK-based CAK using [[CLI management command]]
- Manage generation of a PSK-based CAK

4.1.5 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.

4.1.6 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 generated using a configurable hash function. 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.

4.1.7 Trusted Path/Channels

The TOE supports syslog protocol over TLS v1.2 for secure communication to the audit server. The TOE supports TLS v1.2 for secure communication to LDAP and Radius servers for authentication. The TOE supports local CLI and uses SSH v2 for secure remote administration.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The Security Problem Definition, including the assumptions, may be found in the following documents:

- *collaborative Protection Profile for Network Device*, Version 3.0e, 6 December 2023 [CPP_ND_V3.0E]
- *PP-Module for MACsec Ethernet Encryption*, Version 1.0, 02 March 2023 [MOD_MACsec_V1.0]
- *Functional Package for Secure Shell (SSH)*, Version 1.0, 13 May 2021 [PKG_SSH_V1.0]

That information has not been reproduced here and the CPP_ND_V3.0E/MOD_MACsec_V1.0/ PKG_SSH_V1.0 should be consulted if there is interest in that material.

5.2 Clarification of Scope

The scope of this evaluation was limited to the functionality and assurances covered in the CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0 as described for this TOE in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionality provided by the devices needs to be assessed separately, and no further conclusions can be drawn about their effectiveness.

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarification. 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 assurance activities specified in the CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0 and performed by the Evaluation team).
- 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.
- Apart from the Admin Guides identified in Section 6, additional customer documentation for the specific TOE models was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.
- This evaluation did not specifically search for, nor attempt to exploit, 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 functionality evaluated is scoped exclusively to the security functional requirements specified in the CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0 and applicable Technical Decisions. Any additional security related functional capabilities of the TOE were not covered by this evaluation.

6 Documentation

The following document was provided by the vendor with the TOE for evaluation:

- *Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Common Criteria Supplement Guide*, Version 0.7, August 22, 2025

To use the product in the evaluated configuration, the product must be configured as specified in the Guidance Documentation listed above. Consumers are encouraged to download the configuration guide from the NIAP website to ensure the device is configured as evaluated.

Any additional customer documentation provided with the product, or that is available online, was not included in the scope of the evaluation and, therefore, should not be relied upon when configuring or operating the device as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

The evaluated TOE models and evaluated configuration can be found in Sections 3.1 and 3.2 of this report.

7.2 Excluded Functionality

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

- NTP server
- gRPC is disabled
- telnet is disabled
- MPLS is not evaluated
- SNMP is not evaluated
- Netconf 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 the following proprietary document:

- *Evaluation Technical Report for Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms*, Version 0.6, August 25, 2025

A non-proprietary summary of the assurance activities is provided in the following document:

- *Assurance Activity Report for Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms*, Version 0.7, August 28, 2025

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 to the vendor-provided guidance documentation and ran the tests specified in the CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0. The Independent Testing activity is documented in the AAR, 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 ETR. The reader of this document can assume that all 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.5 and CEM version 3.1 Rev.5. The Evaluation team determined the Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms to be Part 2 extended, and meets the SARs contained in the PP. Additionally, the Evaluation team performed the Assurance Activities specified in the claimed PP/MOD/PKG.

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 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms that are consistent with the Common Criteria, and product security function descriptions that support the requirements.

The Validation team 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 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 ST and Guidance document. Additionally, the Evaluator performed the assurance activities specified in the CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0 related to the examination of the information contained in the TOE Summary Specification.

The Validation team 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.

9.3 Evaluation of Guidance Documents

The Evaluation team applied each 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. All 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 CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0 related to the examination of the information contained in the operational guidance documents.

The Validation team 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.

9.4 Evaluation of Life Cycle Support Activities

The Evaluation team applied each ALC CEM work unit. The Evaluation team found that the TOE was identified.

The Validation team 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 ATE CEM work unit. The Evaluation team ran the set of tests specified by the Assurance Activities in the CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0 and recorded the results in a Test Report, summarized in the ETR and AAR.

The Validation team 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 CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0, and that the conclusion reached by the Evaluation team was justified.

9.6 Vulnerability Assessment Activity

The Evaluation team applied each AVA CEM work unit. The vulnerability analysis is in the proprietary Vulnerability Analysis Report prepared by the evaluator. The vulnerability analysis includes a public search for vulnerabilities.

- The Evaluation team performed a search of the following public vulnerability databases:
- https://nvd.nist.gov/view/vuln.search
- http://cve.mitre.org/cve
- https://www.cisa.gov
- https://www.nokia.com/about-us/security-and-privacy/product-security-advisory/

The Evaluation team performed vulnerability searches using the following key words. The search was performed on August 29, 2025:

- 7750 SR-1 (FP4), 7750 SR-1-24D, 7750 SR-1-48D, 7750 SR-1-46S, 7750 SR-1-92S, 7750 SR-1x-48D, 7750 SR-1x-92S, 7750 SR-1se CPM, 7750 SR-2se CPM-2se, 7750 SR-2s CPM, 7750 SR-14s/7s CPM-s v2 (SR-s CPM-2S), 7750 SR-7/SR-12/SR-12e SR CPM5
- 7250 IXR-R6d/dl CPIOM, 7250 IXR-e CPM (Small), 7250 IXR-R4 CPM, 7250 IXR-R6 CPIOM
- Nokia SR OS, Nokia SR OS 24.10.R3
- TiMOS SMP version 2.5
- Nokia SR Cryptographic Module (SRCM) version 5
- Broadcom BCM82399, Broadcom BCM81392, Broadcom BCM81394, Broadcom BCM81343

- Microsemi VSC8258, Microsemi VSC8490, Microsemi VSC8584
- Nokia E5
- Marvell OCTEON II CN6645 (MIPS64), Marvell OCTEON III CN7340 (MIPS64) , Marvell OCTEON III CN7360 (MIPS64), Marvell OCTEON III CN7890 (MIPS64)
- AMD EPYC3251 (ZEN), AMD EPYC3255 (ZEN)
- Intel Atom C3708 (Goldmont)
- OpenSSL 3.1.7
- OpenSSH 8.9

The Evaluation team conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

The Validation team 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.

9.7 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 followed the procedures defined in the CEM, performed the Assurance Activities in the CPP_ND_V3.0E/MOD_MACsec_V1.0/PKG_SSH_V1.0, 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 instructions in the Guidance document defined in Section 6. No other versions of the TOE and software, either earlier or later, were evaluated.

The evaluated functionality is scoped exclusively to the security functional requirements specified in the ST. Other functionality included in the product was not assessed as part of this evaluation. All other functionalities provided by devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness. Specifically, Section 7.2 defines functionality that was excluded from or not allowed in the evaluated configuration.

Per NIAP Scheme Policy Letter #22, user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date; with such updates properly installed, the product is still considered by NIAP to be in its evaluated configuration.

11 Annexes

Not applicable.

12 Security Target

The ST for this product's evaluation is the *Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Security Target*, Version 1.2, August 22, 2025.

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.
5. *PP-Configuration for Network Devices and MACsec Ethernet Encryption*, 2023-03-29
6. *collaborative Protection Profile for Network Devices*, Version 3.0e, December 06, 2023
7. *PP-Module for MACsec Ethernet Encryption*, Version 1.0, March 2, 2023
8. *Functional Package for Secure Shell (SSH)*, Version 1.0, May 13, 2021
9. *Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Security Target*, Version 1.2, August 22, 2025
10. *Assurance Activity Report for Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms*, Version 0.7, August 28, 2025
11. *Evaluation Technical Report for Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms*, Version 0.6, August 25, 2025
12. *Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms Common Criteria Supplement Guide*, Version 0.7, August 22, 2025
13. *Vulnerability Assessment for Nokia 7750 SR & 7250 IXR, SROS 24.10.R3, MACsec platforms*, Version 0.6, August 29, 2025
14. *Test Plan for Nokia 7250 IXR-E CPM (small)*, Version 1.2, August 25, 2025
15. *Test Plan for Nokia 7250 IXR-R4 CPM*, Version 1.2, August 25, 2025
16. *Test Plan for Nokia 7750 SR1-58D*, Version 1.2, August 25, 2025
17. *Nokia 7750 SR & 7250 IXR, SROS 24,10.R3, MACsec platforms Equivalency Analysis Report*, Version 1.5, July 11, 2025