National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for the

Nokia 7705 SAR Series with SAR OS 21.10R5

Report Number: CCEVS-VR-VID11353-2023

Dated: September 29, 2023

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 Meade, MD 20755-6982

ACKNOWLEDGEMENTS

Validation Team

James Donndelinger

Jerome Myers, PhD

Marybeth Panock

Mike Quintos

The Aerospace Corporation

Common Criteria Testing Laboratory

Shehan Dissanayake

Shivani Birwadkar

Minal Wankhede

Yogesh Pawar

Acumen Security, LLC

Table of Contents

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the Nokia 7705 SAR Series with SAR OS 21.10R5 Target of Evaluation (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 September 2023. 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, 27 March 2020 [NDcPP].

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, 27 March 2020 [NDcPP]. 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 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 Profile 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 Compliance 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 7705 SAR Series with SAR OS 21.10R5
Protection Profile	collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP]
Security Target	Nokia 7705 SAR Series with SAR OS 21.10R5 Security Target
Evaluation Technical Report	Evaluation Technical Report for Nokia 7705 SAR Series with SAR OS 21.10R5
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 2400 Research Blvd, Suite 395, Rockville, MD 20850.
CCEVS Validators	James Donndelinger, The Aerospace Corporation Jerome Myers, PhD, The Aerospace Corporation Marybeth Panock, The Aerospace Corporation Mike Quintos, The Aerospace Corporation

3 Assumptions and Clarification of Scope

3.1 Assumptions

The following assumptions about the operational environment are made regarding its ability to provide security functionality.

- It is assumed that the TOE is deployed in a physically secured operational environment and not subjected to any physical attacks.
- It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration, and support of the TOE.
- The TOE is not responsible for protecting network traffic that is transmitted across its interfaces that is not related to any TOE management functionality or generated data.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- It is assumed that regular software and firmware updates will be applied by a TOE Administrator when made available by the product vendor.
- Administrator credentials are assumed to be secured from unauthorized disclosure.
- It is assumed that the availability of all TOE components is checked as appropriate to reduce the risk of an undetected attack against a TOE component and that auditing is functioning on all TOE components.
- TOE Administrators are trusted to ensure that there is no unauthorized access possible for sensitive residual information on the TOE when it is removed from its operational environment.

3.2 Threats

The following lists the threats addressed by the TOE.

- **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 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.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.

3.3 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that might benefit from additional 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 level of assurance for this evaluation is defined within the Collaborative Protection Profile for Network Devices Version 2.2e (NDcPP), March 23, 2020, including all relevant NIAP Technical Decisions. A subset of the "optional" and "selection-based" security requirements defined in the NDcPP are claimed by the TOE and documented in the ST.

- 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 security functionality 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 Security Target. Any additional security functional capability included in the product were not covered by this evaluation. Further information of excluded functionality can be found in Section 1.8 of the Security Target and Section 7.2 of this Validation Report. All other functionality provided by other devices in the operational environment needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

4 Architectural Information

Note: The following architectural description is based on the description presented in the Security Target.

4.1 TOE Description

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].

The TOE is a physical, non-distributed network device implementing networking functions essential for service adaptation, aggregation and routing over Ethernet and Internet Protocol routing infrastructure. The primary scenario of deployment is for mobile backhaul, fixed to mobile convergence, mission-critical applications and enterprise applications.

Each variant of the TOE is fully contained in a single chassis. The TOE may interact with external servers to implement the functions and services, and may be administered from a local or remote management station, but neither the servers nor the management stations are parts of the TOE.

The TOE implements a set of security functions and security mechanisms consistent with the requirements set in the collaborative Protection Profile for Network Devices (NDcPP) Version 2.2e. These include security audit, cryptographic algorithms and protocols, authentication of users and peer entities and assigning the users to roles, security management, Protection of the TOE and the TSF, controlling access to the TOE, and trusted channels and paths between the TOE and peer entities and between the TOE and users.

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

Each variant of the TOE executes identical software, namely, the Nokia Service Aggregation Router Operating System (SAR OS) Release 21.10R5, and is to be used in accordance with a common security guidance. The TOE models are summarized in Table 2.

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

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

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

Table 2: TOE Models

Platform Description	Processors
7705 SAR-18  # of Cores: 8 Frequency: 600 MHz on SAR-18 CSM module OS: Nokia SAR OS Image Version: 21.10R5	Cavium OCTEON Plus CN5640
7705 SAR-8  # of Cores: 6 Frequency: 800 MHz, on CSMv2 module OS: Nokia SAR OS Image Version: 21.10R5	Cavium OCTEON II CN6335
7705 SAR-X  # of Cores: 8 Frequency: 800 MHz on chassis OS: Nokia SAR OS Image Version: 21.10R5	Cavium OCTEON II CN6640
7705 SAR-H  # of Cores: 2 Frequency: 600 MHz on chassis OS: Nokia SAR OS Image Version: 21.10R5	Cavium OCTEON Plus CN5020
7705 SAR-Hc	Cavium OCTEON II CN6020

Platform Description	Processors
 # of Cores: 2 Frequency: 600 MHz on chassis OS: Nokia SAR OS Image Version: 21.10R5	
7705 SAR-W  # of Cores: 1 Frequency: 500 MHz on chassis OS: Nokia SAR OS Image Version: 21.10R5	Cavium OCTEON Plus CN5010
7705 SAR-Wx  # of Cores: 2 Frequency: 600 MHz on chassis OS: Nokia SAR OS Image Version: 21.10R5	Cavium OCTEON II CN6020
7705 SAR-Ax  # of Cores: 2 Frequency: 600 MHz on chassis OS: Nokia SAR OS Image Version: 21.10R5	Cavium OCTEON II CN6020

4.2 Physical Boundary

The TOE is deployed inside a secure data center or other premises where physical access is effectively controlled. This ensures that only authorized personnel gain physical access to the TOE. Logical access may be through the management station or through the network interfaces. A management station may be local or remote. In addition to the management stations, a CA/CRL Server, AAA Server, Syslog Server and Update Server may be deployed in the same network with the TOE. Access methods to the different management stations and servers are different as are the protocols for protecting network traffic between them and the TOE. The deployment scenario of the TOE is as illustrated in Figure 1.

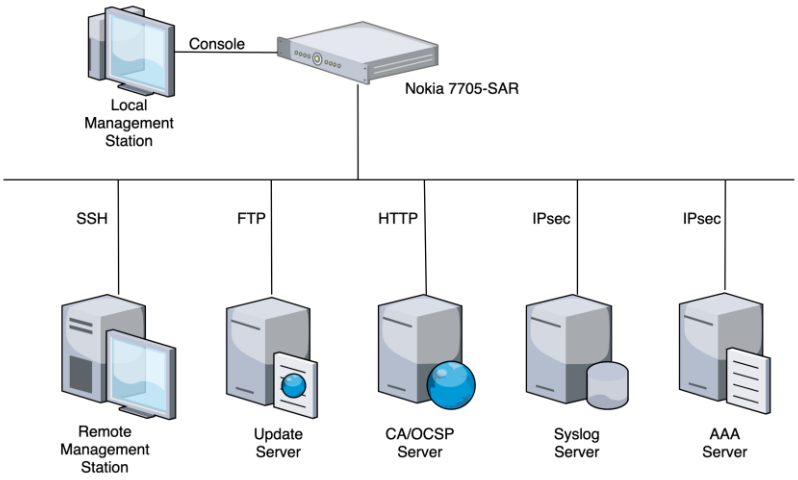

Figure 1 – Representative TOE Deployment

The TOE may be administered locally or remotely. In both methods, the administrative interface is the Command Line Interface (CLI) the TOE software implements for all management functions. If administering the TOE locally, the administrator connects the local management station to the console port of the TOE and operates the TOE in the immediate proximity inside the same data center in which the TOE is deployed. If administering the TOE from a Remote Management Station, the administrator first establishes a Secure Shell (SSH) connection between the Remote Management Station and the TOE, and then proceeds to administer the TOE using the same CLI available to the local administrators from the Local Management Station.

The TOE supports manual upgrading of the TOE software. The administrators load the updates from the developer's web site to a local Update Server or use the developer's update server, then connect the TOE to the Update Server using FTP or SFTP. The software upgrade contains a hash value computed from the image. The hash value shall be verified prior to accepting the upgrade. Therefore, the likelihood of tampering with the TOE software upgrade without detection is very low and there is no need for protection of the connection between the TOE and the Update Server.

To support X.509 certificates with IPsec, the TOE implements a CA/CRL Server used for verifying the certificates and checking their revocation status. As certificates and revocation lists are digitally signed, it is sufficient to connect to them with HTTP. The TOE also may connect to a remote Syslog server for storing audit logs and to an AAA Server storing authentication credentials remotely. Both connections are protected with IPsec.

5 Security Policy

The TOE implements the following security functional requirements:

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

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

5.1 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 over IPsec 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.

5.2 Cryptographic Support

The TOE provides cryptography in support of SSH and IPSEC trusted communications. The following table identifies the cryptographic services per cryptographic library.

Table 3: TOE Cryptography Implementation

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
FCS_CKM.1	RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3	Nokia 7705 SAR OS Cryptographic library	RSA KeyGen (FIPS186-4)	C2023
		Nokia 7705 SAR OS Cryptographic library		C2024
	FFC Schemes using 'safe-prime' groups that meet the following: "NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" and [RFC 3526]	Nokia 7705 SAR OS Cryptographic library	Safe Primes Key Generation Safe Primes Key Verification	A3133
		Nokia 7705 SAR OS Cryptographic library	Safe Primes Key Generation	A3134

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
			Safe Primes Key Verification	
FCS_CKM.2	RSA-based key establishment schemes that meet the following: RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 3447, “Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1”	Nokia 7705 SAR OS Cryptographic library	None	CCTL tested as per the PP/SD Evaluation Activities
	FFC Schemes using “safe-prime” groups that meet the following: ‘NIST Special Publication 800- 56A Revision 3, “Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography” and [RFC 3526]	Nokia 7705 SAR OS Cryptographic library	KAS-FFC-SSC Sp800-56Ar3	A3133
		Nokia 7705 SAR OS Cryptographic library	KAS-FFC-SSC Sp800-56Ar3	A3134
FCS_COP.1/ DataEncryption	AES used in [CBC, CTR] mode and cryptographic key sizes [128 bits, 192 bits, 256 bits]	Nokia 7705 SAR OS Cryptographic library	AES-CBC AES-CTR	C2023
		Nokia 7705 SAR OS Cryptographic library		C2024
FCS_COP.1/ SigGen	For RSA schemes: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS and/or RSASSA-PKCS1v1_5; ISO/IEC 9796-2, Digital signature scheme 2 or Digital Signature scheme 3	Nokia 7705 SAR OS Cryptographic library	RSA SigGen (FIPS186-4) RSA SigVer (FIPS186-4)	C2023
		Nokia 7705 SAR OS Cryptographic library		C2024
FCS_COP.1/ Hash	[SHA-1, SHA-256, SHA-384, SHA-512] and message digest sizes [160, 256, 384, 512] bits	Nokia 7705 SAR OS Cryptographic library	SHS	C2023
		Nokia 7705 SAR OS Cryptographic library		C2024
FCS_COP.1/ KeyedHash	[HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512] and cryptographic key sizes [160-bits, 256-bits,	Nokia 7705 SAR OS Cryptographic library	HMAC-SHA-1 HMAC-SHA-256	C2023

SFR	Algorithm in ST	Implementation name	CAVP Alg.	CAVP Cert #
	384-bits, 512-bits] and message digest sizes [160, 256, 384, 512] bits	Nokia 7705 SAR OS Cryptographic library	HMAC-SHA-384 HMAC-SHA-512	C2024
FCS_RBG_EXT.1	CTR_DRBG (AES)	Nokia 7705 SAR OS Cryptographic library	Counter DRBG	C2023
		Nokia 7705 SAR OS Cryptographic library		C2024

5.3 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.

5.4 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
- Role Based Access Control
- Configurable banners to be displayed at login
- Timeouts to terminate administrative sessions after a set period of inactivity
- Protection of secret keys and passwords

5.5 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.

5.6 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.

5.7 Trusted Path/Channels

The TOE supports IPsec for secure communication to the audit server and with the authentication server. The termination points of the IPsec are the TOE and another IPsec implementation. The TOE supports local CLI and uses SSH v2 for secure remote administration.

6 Documentation

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

- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide 1.0, May 15, 2023
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Basic System Configuration Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Interface Configuration Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Log Events Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Router Configuration Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Services Guide, Edition 01, October 2021
- NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 System Management Guide, Edition 01, October 2021

The documentation listed above are the only documentation that should be trusted to install, administer, or use the TOE in its evaluated configuration. 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 device as evaluated. 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 guides from the NIAP website to ensure the device is configured as evaluated.

7 TOE Evaluated Configuration

7.1 Evaluated Configuration

In the evaluated configuration, the TOE consists of the platform as stated in Section 4.1. The TOE supports secure connectivity with another IT environment device as stated in the Security Target.

Table 4: Required Environmental Components

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

7.2 Excluded Functionality

The following product functionality is not included in the CC evaluation:

- FTP and Telnet and are disabled.
- NTP is not used.
- TACACS+ cryptographic protection of the sessions is not covered by the evaluation but the security of TACACS+ relies on IPsec between the TOE and the AAA Server.
- MPLS and SNMP are not included in the scope of the evaluation.
- MACsec functionality is not supported.

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 Reports for Nokia 7705 SAR Series with SAR OS 21.10R5, which are not publicly available. The Assurance Activities Report 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 vendor-provided guidance documentation and ran the tests specified in the collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP]. 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 5 and CEM version 3.1 rev 5. The evaluation determined the Nokia 7705 SAR Series with SAR OS 21.10R5 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 7705 SAR Series with SAR OS 21.10R5 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 collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP].

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 collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] 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 collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] 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 collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP] 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 collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP], 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. In compliance with AVA_VAN.1, the evaluator examined sources of publicly available information to identify potential vulnerabilities in the TOE. The sources of examined are as follows:

- https://nvd.nist.gov/view/vuln.search
- https://www.nokia.com/
- https://www.suse.com/
- https://www.nokia.com/about-us/security-and-privacy/product-security-advisory/
- https://www.openssl.org/news/vulnerabilities.html

The evaluator examined public domain vulnerability searches by performing a keyword search. The terms used for this search were based on the vendor name, product name, and key platform features leveraged by the product. As a result, the evaluator performed a search using the following keywords:

- Nokia 7705 SAR
- Nokia Service Aggregation Router
- Nokia OS 21.10R5
- OpenSSL 1.1.1g

- OpenSSH 3.5p1
- Cavium OCTEON Plus
- Cavium OCTEON II
- Winpath 3
- Winpath
- strongSwan 5.5.0

The 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 collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP], and that the conclusion reached by the evaluation team was justified. The vulnerability assessment was completed on September 15, 2023.

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 collaborative Protection Profile for Network Devices, Version 2.2e, 27 March 2020 [NDcPP], 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 NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide 1.0, May 15, 2023. No other versions of the TOE and software, either earlier or later were evaluated.

The scope of this evaluation was limited to the functionality and assurances specified in the Security Target. Other functionality included in the product was not assessed as part of this evaluation. The excluded functionality is specified in section 7.2 of this report.

Additional functionality provided by other devices in the operational environment need to be assessed separately and no further conclusions can be drawn about their effectiveness.

All other items and scope issues have been sufficiently addressed elsewhere in this document.

11 Annexes

Not applicable.

12 Security Target

Nokia 7705 SAR Series with SAR OS 21.10R5 Security Target, Version 1.4, September 28, 2023

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. Nokia 7705 SAR Series with SAR OS 21.10R5 Security Target, Version 1.4, September 28, 2023 (ST)
6. NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R5 Common Criteria Admin Guide 1.0, May 15, 2023 (AGD)
    a. NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Basic System Configuration Guide, Edition 01, October 2021
    b. NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Interface Configuration Guide, Edition 01, October 2021
    c. NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Log Events Guide, Edition 01, October 2021
    d. NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Router Configuration Guide, Edition 01, October 2021
    e. NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 Services Guide, Edition 01, October 2021
    f. NOKIA 7705 SERVICE AGGREGATION ROUTER | RELEASE 21.10R1 System Management Guide, Edition 01, October 2021
7. Assurance Activity Report for Nokia 7705 SAR Series with SAR OS 21.10R5, Version 1.3, September 28, 2023 (AAR)
8. Evaluation Technical Report for Nokia 7705 SAR Series with SAR OS 21.10R5, Version 1.3, September 28, 2023 (ETR)
9. Vulnerability Assessment for Nokia Corporation, Nokia 7705 SAR Series with SAR OS 7705 SAR Series with SAR OS 21.10R5, Version 1.2, September 15, 2023 (AVA)
10. Equivalency Analysis for Nokia 7705 SAR Series with SAR OS 21.10R5, Version 1.1, 11 August 2023
11. Test Report for Nokia 7705 SAR Series with SAR OS 21.10R5, Test Evidence for Nokia 7705 SAR-W, Version 1.1, August 11, 2023
12. Test Report for Nokia 7705 SAR Series with SAR OS 21.10R5, Test Evidence for Nokia 7705 SAR-X, Version 1.1, August 11, 2023