CSEC

Swedish Certification Body for IT Security

Certification Report - Nokia 7-Series Service Router Operating System (SR OS) Family

Issue: 1.0, 2022-jun-03

Authorisation: Ulf Noring, Lead Certifier , CSEC

SWEDAC · ACKREDITERING ·
Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1 Executive Summary

The TOE is the Nokia 7-Series Service Router Operating System (SR OS) Family consisting of the:

a. Nokia 7x50 Service Router Operating System (SR OS), v21.10.R1.

b. Nokia Service Aggregation Router Operating System (SAR OS), v21.10.R1.

c. Nokia Service Access Switch Operating System (SAS OS), v21.9.R1.

The TOE consists of the SR OS software running on various router and switch platforms and models as listed below.

Platform	Model(s)	Operating System
7750 Service Router (SR)	SR-7, SR-12, SR-12e, SR-1s, SR-2s, SR-a4, SR-a8	SR OS v21.10.R1
7250 Interconnect Routers (IXR)	IXR-e, IXR-R6, IXR-R4, IXR-10, IXR-6, IXR-s	
7705 Service Aggregation Router (SAR)	SAR-18, SAR-8, SAR-X, SAR-Ax, SAR-H, SAR-Hc, SAR-Hm, SAR-Hmc.	SAR OS v21.10.R1
7210 Service Access Switch (SAS)	SAS-R12, SAS-R6, SAS-MXP, SAS-D, SAS-Dxp , SAS-S, SAS-Sx, SAS-K30, SAS-K12, SAS-K5	SAS OS v21.9.R1

The evaluation has been performed by Combitech AB and EWA-Canada. Remote Site Visit at the developer's site in Ottawa, Canada, was performed.

The evaluation was completed on 2022-05-30. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

Combitech AB is a licensed evaluation facility for Common Criteria under the Swedish Common Criteria Evaluation and Certification Scheme. Combitech AB is also accredited by the Swedish accreditation body according to ISO/IEC 17025 for Common Criteria.

EWA-Canada operates as a foreign location for Combitech AB within the scope of the Swedish Common Criteria Evaluation and Certification Scheme.

The certifiers monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports, and by observing site-visit and testing. The certifiers determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 3 augmented by ALC_FLR.1.

The technical information in this report is based on the Security Target (ST) and the Final Evaluation Report (FER) produced by Combitech AB.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

2 Identification

Certification Identification	
Certification ID	CSEC2020023
Name and version of the certified IT product	Nokia7-Series Service Router Operating System (SR OS) Family: SR OS v21.10.R1 SAR OS v21.10.R1 SAS OS v21.9.R1
Security Target Identification	Security Target for Nokia 7-Series Service Router Operating System (SR OS) Family, Nokia, 2022-05-16, document version 1.1.
EAL	EAL 3+ ALC_FLR.1
Sponsor	Nokia Canada Inc.
Developer	Nokia Canada Inc.
ITSEF	Combitech AB
Common Criteria version	3.1 release 5
CEM version	3.1 release 5
QMS version	2.1.1
Scheme Notes Release	18.0
Recognition Scope	CCRA, SOGIS, EA/MLA
Certification date	2022-06-03

3 Security Policy

- Audit
- Identification & Authentication (I&A)
- Security Management
- TOE Access
- User data protection (Information flow control)

3.1 Audit

Event logging controls the generation, dissemination and recording of system events for monitoring status and troubleshooting faults within the system.

Audit also keeps track of the activity of an administrator who has accessed the network. The type of audit information recorded includes a history of the commands executed, the amount of time spent in the session, the services accessed, and the data transfer size during the session.

3.2 Identification & Authentication (I&A)

SR OS identifies and authenticates individual users by validating an administrator's username and password. Administrators are identified and authenticated via local authentication, RADIUS, or TACACS+. All authentication methods are available on each management interface. SR OS also provides authentication failure handling on the Console and the ability for the administrator to define password complexity requirements.

3.3 Security Management

SR OS implements authorization features, which allow the administrator to access and execute commands at various command levels based on profiles assigned to the administrator. The Administrator configures system security and access functions and logging features using CLI syntax and command usage to configure parameters.

3.4 TOE Access

Mechanisms place controls on Administrators' sessions. An administrator-configurable message is displayed before establishing a user session. Local and remote Administrator's sessions are dropped after an Administrator-defined time period of inactivity. Dropping the connection of a local and remote session (after the specified time period) reduces the risk of someone accessing the local and remote machines where the session was established, thus gaining unauthorized access to the session.

3.5 User data protection (Information flow control)

The SR OS enforces an UNAUTHENTICATED SFP whereby the network packets sent through the TOE are subject to router [information flow control] rules setup by the administrator. The Quality of Service (QoS) and Access Control List (ACL) filter capabilities of the SR OS can mitigate DoS activity.

The SR OS enforces an AUTHENTICATED SFP whereby information is passed via application proxy (Console, NSP, SNMP). Users must first be granted access by the administrator and then authenticated in order to access the router by Console, NSP, or SNMP. Management Access Filters (MAF) can be used to prevent Denial of Service (DoS) attacks.

The SR OS enforces an EXPORT SFP whereby information events are sent from the TOE to SNMP trap, Syslog, and RADIUS/TACACS+ destinations.

4 Assumptions and Clarification of Scope

4.1 Usage and Environmental Assumptions

The Security Target [ST] makes nine assumptions on the usage and environment of the TOE.

A.ADMINISTRATOR It is assumed that authorized administrators are not careless, wilfully negligent, or hostile and will follow and abide by the instructions provided by the TOE documentation, including the administrator guidance, and will periodically check the audit record; however, they are capable of error. It is further assumed that personnel will be trained in the appropriate use of the TOE to ensure security.

A.PHYSICAL It is assumed that the operational environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

A.LOCATION It is assumed that the processing resources of the TOE will be located within controlled access facilities which will prevent unauthorized physical access.

A.CONNECTIVITY It is assumed that the trusted remote systems that communicate with the TOE, except for the network traffic/data interface, are attached to the internal (trusted) network. This includes: (1) the RADIUS, TACACS+ server; (2) the NSP server; (3) system with SCP interface; (4) the SNMP, Syslog servers; and (5) the NTP server. The Network traffic/data interface is attached to internal and external networks. Console Access is via RS-232, a direct local connection in the same physical location as the TOE.

A.GENPURPOSE It is assumed that there are no general purpose computing capabilities (e.g., the ability to execute arbitrary code or applications) and storage repository capabilities on the TOE.

A.EXT_AUTHORIZATION It is assumed that external authentication services will be available to the TOE via either RADIUS, TACACS+, or both, based on defined Internet Engineering Task Force (IETF) standards.

A.INTEROPERABILITY It is assumed that the TOE functions with the external IT entities shown in Figure 1 and with other vendors’ routers on the network and meets Request for Comments (RFC) requirements for implemented protocols.

A.TIMESTAMP It is assumed that the Operational Environment provides the TOE with the necessary reliable time stamp. External Network Time Protocol (NTP) services will also be available to provide external time synchronization.

A.TRUSTED_COMM It is assumed that the Operational Environment will provide trusted communications with the following trusted systems: NSP server, system with SCP interface/remote CLI, SNMP server. It is expected that the operational environment:

a. provides the TOE with the necessary trusted interfaces. Remote management traffic (to/from the TOE) will be protected using SNMP, SSH or SCP (secure copy). Remote telnet and FTP will be disabled.

b. will protect remote administrative sessions from eavesdropping. The Operational environment will provide a means to ensure that administrators are not communicating with some other entity pretending to be the TOE when supplying identification and authentication data.

c. will protect communications with remote external IT entities. The operational environment will ensure that the communication channel is logically distinct from other communication channels.

4.2 Clarification of Scope

The Security Target contains five threats, which have been considered during the evaluation.

T.AUDIT Actions performed by administrators (modification of TOE and network infrastructure and service layer system security configuration/parameters) may not be known to the administrators due to actions not being recorded (and time stamped) or the audit records not being reviewed prior to the machine shutting down, or an unauthorized administrator modifies or destroys audit data.

T.TSF_DATA A malicious administrator may gain unauthorised access to inappropriately view, tamper, modify, or delete TOE Security Functionality (TSF) data.

T.MEDIATE An unauthorized entity may send impermissible information through the TOE which results in the exploitation (e.g., destruction, modification, or removal of information and/or other resources), and/or exhaustion of resources on the network (e.g., bandwidth consumption or packet manipulation).

T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session and view and change the TOE security configuration.

T.UNAUTH_MGT_ACCESS An unauthorized user gains management access to the TOE and views or changes the TOE security configuration.

The Security Target contains three Organisational Security Policies (OSPs), which have been considered during the evaluation.

P.CONSOLE In the deployed configuration of the TOE in its intended environment, the primary means of administering the TOE during normal operations will be via CLI accessed over the local Console or SSH.

P.DEPLOYED_CONFIG The deployed configuration of the TOE in its intended environment shall be at least as restrictive as the baseline evaluated configuration defined herein and will be configured in accordance with guidance documentation.

P.USERS The TOE is administered by one or more Administrators who have been granted rights to administer the TOE. All administrators are "vetted" to help ensure their trustworthiness, and administrator connectivity to the TOE is restricted. Non-administrative entities may have their packets routed by the TOE, but that is the extent of their authorization to the TOE's resources.

5 Architectural Information

The TOE consists of software for the 7x50 IXR/SR, 7705 SAR and 7210 SAS platforms.

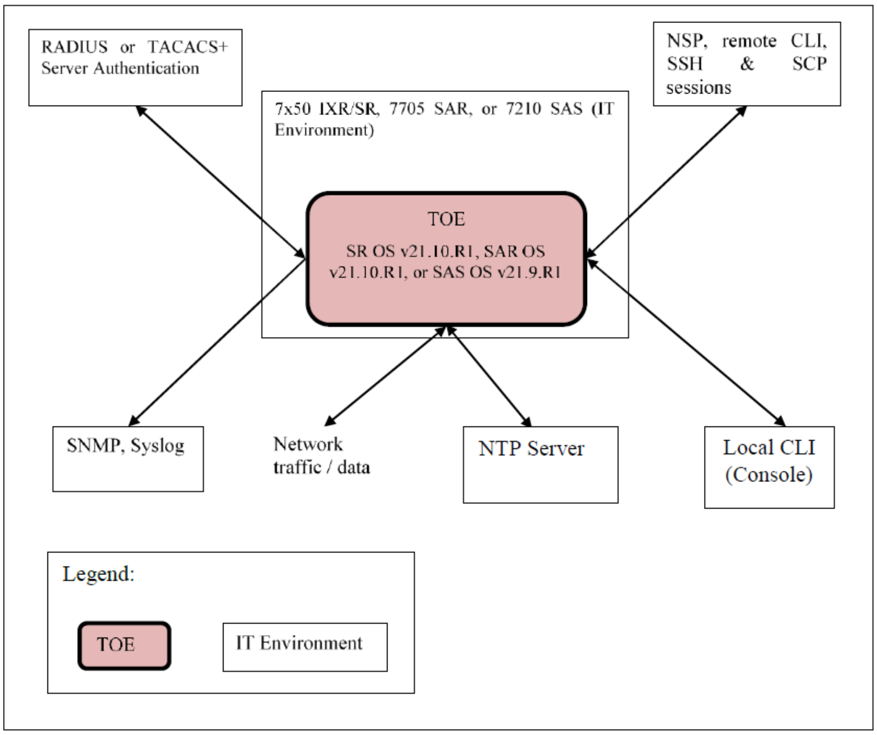
RADIUS or TACACS+ Server Authentication
NSP, remote CLI, SSH & SCP sessions
7x50 IXR/SR, 7705 SAR, or 7210 SAS (IT Environment)
TOE
SR OS v21.10.R1, SAR OS v21.10.R1, or SAS OS v21.9.R1
SNMP, Syslog
Network traffic / data
NTP Server
Local CLI (Console)
Legend:
TOE
IT Environment

Figure 1 TOE Boundary

The physical boundary is the SR OS operating system (i.e., SR OS v21.10.R1, SAR OS v21.10.R1, or SAS OS v21.9.1R1) located on a solid state memory card. The SR OS runs on various hardware platforms but the hardware platforms are excluded. The TOE’s operational environment requires the following systems be on an internal trusted network: a RADIUS or TACACS+ server for authentication/authorization services, the NSP for limited remote administration, local Console access for most administration, SNMP/Syslog servers for logging, and a Network Time Protocol (NTP) server for external time synchronization.

The TOE is comprised of the following subsystems:

a. Management Plane subsystem – provides configuration control and the connection of statistics and state information for reporting. This subsystem includes Authentication, Authorization, and Accounting, CLI, SNMP, and Logging modules;

b. Control Plane subsystem – handles the dynamic protocols for the exchange of (reachability, topological, and resource state) information, allowing for an accurate forwarding operation; see Security Best Practices and Hardening Guide, Control Plane Security. The Control Plane performs access decisions on control and management traffic (CPM/CSM filter and MAF) and implements routing and MPLS protocols.

c. Data Plane subsystem – handles the forwarding of customer data or service data through the system and provides other planes with statistics and state information; see Security Best Practices and Hardening Guide, Data Plane Security. The Data Plane implements QoS policies, ACL policies, and Filter policies.

d. Platform subsystem – manages the overall hardware system (chassis management) and provides the basic tools for other subsystems to obtain information and communicate with other subsystems as well as the interaction with outside elements.

6 Documentation

7-Series Service Router Operating System (SROS) Family Supplemental Common Criteria Guidance, Nokia, 2022-03-21, document version 1.0

Detailed instructions for each model can be found in the Security Target [ST], section 1.7.

7 IT Product Testing

7.1 Developer Testing

The developer performed both manual tests and ran automatic test suites. The developer's testing covers the security functional behaviour of all TSFIs and SFRs as well as the interactions of the subsystems.

7.2 Evaluator Testing

The evaluator repeated a number of the developer's automatic tests script suites for each of the three platforms.

The evaluator repeated also two of the developer's manual test cases for each of the three platforms. The test cases were chosen to cover the different Security Functions defined in [ST] chapter 7.

Individual and penetration test cases were devised. The tests included:

- TOE installation and configuration
- Configuring MAF filter
- RADIUS authentication
- Traffic filters
- SNMP trap target
- Access banner

The evaluator used the same test-bed as the developer, which is a network with six nodes. A test-bed server contains the auto-test environment, the test scripts, and a variety of tools that were used for testing (i.e. DHCP server, RADIUS server, TACACs server, SNMP agent, etc.). A traffic generator (IXIA) is also connected as well as terminal servers, hubs, IP-controlled power bars, etc. The network is fully meshed, i.e. each node is cabled to every other node, with multiple parallel links between a sub-set of nodes. Similar test-beds are used for all TOE families.

Tests were run manually from the test-bed server, a terminal server for remote CLI interaction and an external laptop. Automatic test scripts were also run from the test-bed server and the results, Pass/Fail, were examined in the regression test database.

All tests were executed by Nokia personnel. The Combitech evaluator supervised more than 60% of the tests remotely from Stockholm. The supervised tests were chosen to cover different security capabilities on all three platforms. Tests on platforms 7x50 and 7705 were done at the Nokia site in Ottawa, Canada, and on platform 7210 at the Nokia site in Bangalore, India.

The actual results of all test cases were consistent with the expected test results and all tests were judged to pass.

7.3 Penetration Testing

Penetration test were performed, including

- Port scanning
- Vulnerability scanning
- SSH protocol compliance

Port scans were ran after installation and configuration had been done according the guidance documentation. The purpose was to check that no unexpected ports were opened unfiltered and no unexpected services available. The Nmap (www.nmap.org) port scan tool was used. Four different modes were used: TCP Connect, TCP SYN, UDP, and IP protocol scans. All possible 65535 ports were scanned for TCP/UDP.

Nessus (www.tenable.com) network vulnerability scans were run. No high severity issues were found.

It was verified that the SSHv2 channel was encrypted and that no older versions of the protocol could be used.

All penetration testing had negative outcome, i.e. no vulnerabilities were found.

8 Evaluated Configuration

The evaluated configuration for the TOE must include the following enabled/disabled/configured (all other services, protocols and settings are excluded from the evaluated configuration):

a. Enable SR OS (CLIENT-side) for:

(1) RADIUS or TACACS+ server authentication/ authorization services;

(2) local Console access for most administration;

(3) SNMP/Syslog servers for logging; and

(4) Network Time Protocol (NTP) server for external time synchronization;

b. Enable Routing protocols from this set:

(1) OSPFv2;

(2) IS-IS;

(3) BGP-4; and

(4) MPLS (LDP, RSVP-TE);

c. Ensure Telnet and FTP remain disabled;

d. Use SNMPv3 only;

e. Configure MAF filters on the IXR/SR, SAR, and SAS devices to restrict access to management ports on the device;

f. Configure MAF filters on IXR/SR, and SAR devices for protection of the CSM/CPM by restricting traffic;

g. Configure Border Gateway Protocol (BGP) and Label Distribution Protocol (LDP) Time to Live (TTL) Security on IXR/SR;

Application Note: BGP is not included in the scope for SAR or SAS for this Evaluation. These devices can support BGP as part of a VPRN (label distribution) and as an exterior protocol for VPRN (eBGP). But the 7705 SAR and the 7210 SAS do not provide typical boarder gateway functions such as RR, iBGP, eBGP for traditional ISP type boundaries.

h. Enforce/enable/configure a strong password policy;

i. Disable sending events to a console destination. The console device is not be used as an event log destination. A log created with the console type destination displays events to the physical console device. Events are displayed to the console screen whether an administrator is logged into the console or not; and

j. Use SSHv2 only (SSHv1 is not allowed)

The following features of the SR OS product family are excluded from the evaluated configuration.

1. The use of Telnet and FTP.

2. The use of the Netconf server.

3. The use SNMPv1 and SNMPv2.

4. The use of gRPC.

5. The use of SSHv1.

6. SR OS is able to function as an NTP server; however that capability is excluded from the evaluated configuration. (The use of NTP/SNTP server mode and multicast/broadcast mode are excluded.).

7. Use of the Model-Driven Command Line Interface (MD-CLI). While there are no known issues with the MD-CLI, this administrative interface was not tested during the evaluation.

The following features of the SR OS product family are outside the evaluated configuration. Their use is allowed in the evaluated configuration, but the features have not been tested.

1. The 7750 SR offers service providers and enterprises differentiated services, from Internet access to multipoint Virtual Private Network (VPN) over a single network infrastructure. VPN is a capability of the SR OS; however, it is defined outside the TOE and was not evaluated.

2. High availability is an important feature in service provider routing systems. Downtime can be very costly, and, in addition to lost revenue, customer information and business-critical communications can be lost. High availability is the combination of continuous uptime over long periods (Mean Time Between Failures (MTBF)) and the speed at which failover or recovery occurs (Mean Time To Repair (MTTR). Network and service availability are critical aspects when offering advanced IP services which dictates that IP routers that are used to construct the foundations of these networks be resilient to component and software outages. The high availability feature is not in the scope of the evaluated configuration.

3. SSH/SCP secure communications is a capability of the SR OS; however, the underlining cryptographic protocols and associated cryptographic functionality are defined outside the TOE and part of the TOE’s operational environment and not evaluated.

4. Border Gateway Protocol (BGP) is not in the scope of the evaluated configuration.

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Basic.

The certifiers reviewed the work of the evaluators and determined that the evaluation was conducted in accordance with the Common Criteria [CC]. The evaluators' overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class / Family	Component	Verdict
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security objectives	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Derived security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Life-cycle support	ALC	PASS
Authorisation controls	ALC_CMC.3	PASS
Implementation representation CM coverage	ALC_CMS.3	PASS
Delivery procedures	ALC_DEL.1	PASS
Identification of security measures	ALC_DVS.1	PASS
Developer defined life-cycle model	ALC_LCD.1	PASS
Flaw reporting procedure	ALC_FLR.1	PASS
Development	ADV	PASS
Security Architecture description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.3	PASS
Architectural design	ADV_TDS.2	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Analysis of coverage	ATE_COV.2	PASS
Testing: Basic design	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - Sampling	ATE_IND.2	PASS
Vulnerability assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.2	PASS

10 Evaluator Comments and Recommendations

None.

11 Bibliography

ST — Security Target for Nokia 7-Series Service Router Operating System (SR OS) Family, Nokia, 2022-05-16, document version 1.1.

CCADM — 7-Series Service Router Operating System (SROS) Family Supplemental Common Criteria Guidance, Nokia, 2022-03-21, document version 1.0

CCpart1 — Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1 revision 5, CCMB-2017-04-001

CCpart2 — Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1 revision 5, CCMB-2017-04-002

CCpart3 — Common Criteria for Information Technology Security Evaluation, Part 3, version 3.1 revision 5, CCMB-2017-04-003

CC — CCpart1 + CCpart2 + CCpart3

CEM — Common Methodology for Information Technology Security Evaluation, version 3.1 revision 5, CCMB-2017-04-004

EP-002 — EP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34.0

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.1.1	2022-02-25	None
2.1	2022-01-18	None
2.0	2021-11-24	None
1.25	2021-06-17	None
1.24.1	Application	Original version

A.2 Scheme Notes

The following Scheme Notes have been considered during the evaluation:

- Scheme Note 15 - Testing
- Scheme Note 18 - Highlighted Requirements on the Security Target
- Scheme Note 22 - Vulnerability assessment
- Scheme Note 31 - New procedures for site visit oversight and testing oversight