



A Certification Body of atsec information security AB
under the EUCC scheme

Certification Report - Nokia Lightspan Access Node MF-2

Certification ID EUCC-3089-2026-002

Certification Body ID 3089

Version 1.0

Author David Hedberg

atsec information security AB
Svärdvägen 23
SE-182 33 Danderyd
Phone: +46 8 55 110 400
www.atsec.com

©2026 atsec information security AB

The objective of the certification report is to provide detailed and practical security information about the ICT product or protection profile for any interested parties. The report does not contain any protected information. This report is based on the Evaluation Technical Report/s.

Disclaimer: The certification or certificate is entirely related to the cybersecurity certification requirements of the product at the moment of issuance of the certificate. It is not related to the product itself.

The certification is not an endorsement of the product, the package or anything else related to the product. It only expresses that the cybersecurity related material and information of the product meets the requirements of this certification related information. There are no warranties about fit for purpose or merchantability, absence of defects, errors, accuracy, non-infringement of intellectual property rights, consumer rights and any other related rights. The issuer of the certification or the cybersecurity certification scheme owner are under no circumstances liable for any direct, indirect, material, technical and IT functionality related or moral damages of any kind arising out of the product for non-use, or use.

Neither will any loss of goodwill, work stoppage, computer failure or malfunction, loss or damages, amendments, misuse, abuse, alteration, destruction, theft, ransom or any other form of unauthorised access to data or any commercial damage generate liability to the issuer of the certificate or the designer of the certification scheme or any other organisation that recognises or gives effect to this certificate, except for gross negligence or wilful misconduct caused by natural persons working under these institutions.

©2026 atsec information security AB

Table of Contents

1 Executive Summary 5
2 Identification of the ICT product 7
2.1 System Requirements 7
2.2 Contact Information 7
2.2.1 Holder of Certificate 7
2.2.2 Certification Body 7
3 Security Policies 9
3.1 Security Audit 9
3.2 Cryptographic Support 9
3.3 Identification and Authentication 9
3.4 Security Function Management 9
3.5 Protection of the TSF 9
3.6 TOE Access 9
3.7 Trusted Path / Channels 9
3.8 Management Access 10
4 Vulnerability handling and Assurance Continuity 11
4.1 Assurance Continuity 11
4.2 Patch Management 11
5 Assumptions and Clarification of Scope 12
5.1 Usage Assumptions 12
5.2 Environment Assumptions 12
5.3 Threats 13
5.4 Organisational Security Policies (OSP) 14
6 Architectural Information 16
7 Supplementary Cybersecurity Information 17
7.1 Documentation 17
8 ICT Product Evaluation 18
8.1 Assurance Components 18
8.2 State-of-the-Art Documents and Evaluation Criteria 18
8.3 Evaluated Configuration 18
8.4 Developer Testing 19
8.5 Evaluator Testing 19
8.6 Penetration Testing 19
9 Results of the Evaluation 20

©2026 atsec information security AB

9.1 Summary 20
9.2 Result 21
10 Certificate Information 22
11 Comments and Recommendations 23
12 Reference to the Security Target 24
13 Glossary 25
14 Bibliography 26

©2026 atsec information security AB

1 Executive Summary

The TOE that is the subject of this Certification Report is the Lightspan Access Node MF-2 running Lightspan 25.12 (SW-build 2512.636).

The developer of the TOE is Nokia Solutions and Networks Oy.

The Nokia Lightspan Access Node MF is a network device that serves as the connection point between the end-user's equipment (like home routers or business gateways) and the core network of a telecom provider. The Optical Network Unit (ONU) in conjunction with the Lightspan Fiber Access Node (OLT), form a fiber access network capable of delivering high-quality voice, video, and data services to both single-family or multi-dwelling residential subscribers and business subscribers. The TOE software runs on the dedicated Lightspan Access Node MF-2 hardware.

The TOE is the software which consists of several standalone Network Elements (NE) which are:

- a shelf Network Element (SHELF-NE) providing common equipment, software, alarm and log management.
- an Aggregation Switch (AS) of the IHUB Network Element (AS-NE) providing the switching and routing functionalities.
- multiple (O)LT Network Elements (LT-NE) providing xPON or P2P transport and forwarding functionality.

The physical scope of the TOE is the software components listed above and the guidance document in the table below:

Guidance documentation	Identification/Reference
Lightspan Security Hardening guide	3JL-43000-ACAA-RJZZA
Customer Release Note	3TJ-00170-MAAA-FMZZB
Lightspan Access Node MF Release 25.12 System Description	3HH-13800-IAAA-TQZZA 22
Software package guide for 25.12	3HH-14266-AAAA-RJZZA 32
User Safety and Installation Manual for MF-2	3HH-90465-AAAA-RJZZA 21
Customer Documentation Package (package containing all the provided OAM Manuals): • Lightspan MF-2 Reference Configurations • Lightspan MF-2/LMNT-B OAM Manual • Lightspan MF-2/LMNT-B IHUB OAM Manual • Lightspan MF-2/LMNT-B Alarms • Lightspan MF-2/LMNT-B IHUB Alarms • LMNT-B eCLI Command Guide	3HH-92611-FAAA

Table 1: Guidance documents

The evaluation was performed by atsec information security AB, located at Svärdvägen 23, 182 33 Danderyd, Stockholm, Sweden. atsec information security AB is accredited according to ISO/IEC 17025 by the Swedish accreditation body Swedac with accreditation number 1937.

The evaluation has been completed on EAL3, augmented with ALC_FLR.2. This corresponds to [EUCC] level "Substantial", as AVA_VAN.2 has been applied. See a description of the evaluation in chapter 8 of this report, along with a summary of the results of the evaluation in chapter 9.

The [ST] does not claim conformance to any Protection Profile.

The [ST] has identified eight assumptions. The TOE relies on these assumptions to properly counter the eight defined threat and to fulfil the OSP that has also been defined. See chapter 5 of this report for further information regarding the specific assumptions, threat, and OSP.

The evaluation was completed in July, 2026. The evaluation was conducted in accordance with the Common Methodology for Information Technology Security Evaluation, CEM:2022, revision 1 [CEM], and corresponding Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, parts 1-5 [CC].

After reviewing the work of the evaluator, the Certification Body has issued the initial certificate for Nokia Lightspan Access Node MF-2 version 25.12 on the 10th of September, 2026. The validity period is 5 years, and the certificate is therefore valid until 10th of September, 2031. The unique identifier of the certificate is **EUCC-3089-2026-002**.

The certification procedures were conducted in line with the provisions and requirements of the [EUCC].

©2026 atsec information security AB

2 Identification of the ICT product

The TOE for this certification is Nokia Lightspan Access Node MF software version 25.12.

The following components make up the TOE:

Type	Reference	Version
Software	Nokia Lightspan Access Node MF	25.12

Table 2: Components

Along with the TOE, a set of guidance documents is provided.

See section 7 of this report for more information regarding the Supplementary Cybersecurity Information, as required by the [CSA].

2.1 System Requirements

The TOE software runs on the dedicated Lightspan Access Node MF-2 hardware and the following components can be found in the operating environment of the TOE on systems other than those hosting the TOE:

- Audit server
- RADIUS server
- Access Controller

2.2 Contact Information

2.2.1 Holder of Certificate

Developer Name	Nokia Solutions and Networks Oy
Address	Karakaari 7 02610 Espoo, Finland P.O. Box 226, FI-00045 Nokia Group
Contact	portal.support@nokia.com
Website link for Supplementary Cybersecurity Information	https://www.nokia.com/we-are-nokia/security/products/cvd/ https://www.nokia.com/support/ https://partners.nokia.com/English/

2.2.2 Certification Body

Name	atsec information security AB
Address	Svärdvägen 23 182 33 Danderyd Sweden
Contact	cb@atsec.com

©2026 atsec information security AB

ITSEF	atsec information security AB
NCCA	Swedish Defence Material Administration (FMV)

©2026 atsec information security AB

3 Security Policies

3.1 Security Audit

The TOE records audit events for authentication attempts and administrative operations. Each audit record contains the date and time of the event, type of event, subject identity (user, device or process) and outcome (success or failure).

The TOE writes audit records can be stored locally. When the local audit storage exceeds a maximum size, the TOE overwrites the oldest audit records. The TOE can be configured to transmit the audit records to a specified, external Syslog server.

3.2 Cryptographic Support

All cryptographic operations, including algorithms and key generation used by the TOE are provided by cryptographic module (OpenSSL). OpenSSL implements the Transport Layer Security (TLS) protocol and cryptographic algorithms. The following table summarizes the cryptographic algorithms implemented in OpenSSL.

3.3 Identification and Authentication

The TOE identifies individual administrative users by user name and authenticates them by passwords or public key. Both authentication methods are allowed by default. The administrator can configure the allowed authentication methods for users of the system. The administrator can create any user and have the user assigned to specific access-groups in line with the intended privilege levels of the created user.

3.4 Security Function Management

The user privileges are applied for every management user access to the database (configuration and/or state) of the TOE. The rules are applied irrespective of the management protocol (CLI, NETCONF) or the underlying security protocol (SSH, TLS). The TOE provides user privileges level access authorization, Role Based Access Control (RBAC) based on a simplification of the RFC8341 Network Configuration Access Control Model (NACM). For ease-of-use and simplification, predefined domains (groups) with assigned rules (read-only/read-write/execute) have instantiated on the Lightspan Access Node.

3.5 Protection of the TSF

The TOE is designed to protect critical security data, including keys and passwords. Sensitive cryptographic keys are stored in the TOE's configuration files. The TOE does not offer an interface to retrieve the contents of its configuration files. Passwords are stored in a salted hashed format.

3.6 TOE Access

The system provides the ability of an administrator user to configure a disconnection time for idle CLI or NETCONF session connections. It is possible to configure the maximum idle time. The administrative users can also actively terminate their session connections (log out).

3.7 Trusted Path / Channels

The TOE secures administrative traffic (i.e., administrators connecting to the TOE in order to configure and maintain it), and offers the establishment of TLS sessions with external log servers in the operational environment for protection of audit records in transfer. The TOE acts as a TLS client.

3.8 Management Access

The TOE provides separation of management traffic from the control and data traffic. The TOE provides a specific management VLAN, which enforces traffic separation. Any management access to the Lightspan Access Node via a VLAN which is not the management VLAN is not possible. Such traffic is dropped.

©2026 atsec information security AB

4 Vulnerability handling and Assurance Continuity

The following policy regarding vulnerability handling has been identified as applicable to the TOE:

- Product Life Cycle Support, Nokia Solutions and Networks Oy, document ID 3HH-03851-0080-DFZZA

4.1 Assurance Continuity

This is an initial certification, and an assurance continuity policy was not provided.

4.2 Patch Management

Patch Management is not applicable to this certification.

5 Assumptions and Clarification of Scope

The [ST] contains nine assumptions and eight threats.

The assumptions are not covered by the TOE itself, but instead require Security Objectives to be fulfilled by the Operational Environment.

5.1 Usage Assumptions

The [ST] makes two assumptions for usage of the TOE.

Assumption	Description
A.TRUSTED_ADMINISTRATOR	The administrator(s) for the TOE are assumed to be trusted and to act in the best interest of security for the organization. This includes appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have sufficient strength and entropy and to lack malicious intent when administering the device. The TOE is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
A.REGULAR_UPDATES	The TOE firmware and software is assumed to be updated by an Administrator on a regular basis in response to the release of product updates due to known vulnerabilities.

5.2 Environment Assumptions

The [ST] makes seven assumptions on the operational environment of the TOE.

Assumption	Description
A.PHYSICAL_PROTECTION	The TOE is assumed to be physically protected in its operational environment and not subject to physical attacks that compromise the security or interfere with the device’s physical interconnections and correct operation. This protection is assumed to be sufficient to protect the device and the data it contains.
A.LIMITED_FUNCTIONALITY	The device is assumed to provide networking functionality as its core function and not provide functionality/services that could be deemed as general purpose computing. For example, the device should not provide a computing platform for general purpose applications (unrelated to networking functionality).
A.RESIDUAL_INFORMATION	The Administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) on networking equipment when the equipment is discarded or removed from its operational environment.
A.NO_THRU_TRAFFIC_PROTECTION	A standard/generic TOE does not provide any assurance regarding the protection of traffic that traverses it. The intent is for the TOE to

©2026 atsec information security AB

	protect data that originates on or is destined to the device itself, to include administrative data and audit data.
A.ADMIN_CREDENTIALS_SECURE	The Administrator’s credentials (private key) used to access the TOE are protected by the platform on which they reside.
A.NTP_SOURCE	The TOE is assumed to have reliable NTP sources available in the operational environment.
A.PLATFORM_ENTROPY	The platform provides seed material of sufficient quality and quantity to initialize and reseed the TOE’s deterministic random bit generator.

5.3 Threats

The [ST] outlines eight threats to the TOE.

Threat	Description
T.UNAUTHORIZED_ADMINISTRARTOR_ACCES	Threat agents may attempt to gain Administrator access to the TOE by nefarious means such as masquerading as an Administrator to the device, 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. Successfully gaining Administrator access allows malicious actions that compromise the security functionality of the device and the network on which it resides.
T.WEAK_CRYPTOGRAPHY	Threat agents may exploit weak cryptographic algorithms or perform a cryptographic exhaust against the key space. Poorly chosen encryption algorithms, modes, and key sizes will allow attackers to compromise the algorithms, or brute force exhaust the key space and give them unauthorized access allowing them to read, manipulate and/or control the traffic with minimal effort.
T.UNTRUSTED_COMMUNICATION_CHANNELS	Threat agents may attempt to target TOE that does not use standardized secure tunnelling protocols to protect the critical network traffic. Attackers may take advantage of poorly designed protocols to successfully perform man-in-the-middle attacks, replay attacks, etc. Successful attacks will result in loss of confidentiality and integrity of the critical network traffic, and potentially could lead to a compromise of the TOE itself.
T.WEAK_AUTHENCTICATION_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 TOE 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 TOE 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 TOE 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. Threat agents may also be able to take advantage of weak administrative passwords to gain privileged access to the device.
T.MANAGEMENT_TRAFFIC	Threat agents may attempt to gain access to the administration traffic through the user traffic. This could allow an attacker to perform malicious actions that compromise the security functionality of the TOE and the network on which it resides.

The threat, as outlined in the [ST], is countered by the TOE. The evaluation did not uncover any threats to the TOE that the TOE does not counter.

As such, there are no threats to the ICT product not countered by the evaluated security functions of the product according to the intended use.

5.4 Organisational Security Policies (OSP)

The [ST] outlines one Organisational Security Policy (OSP):

OSP	Description

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

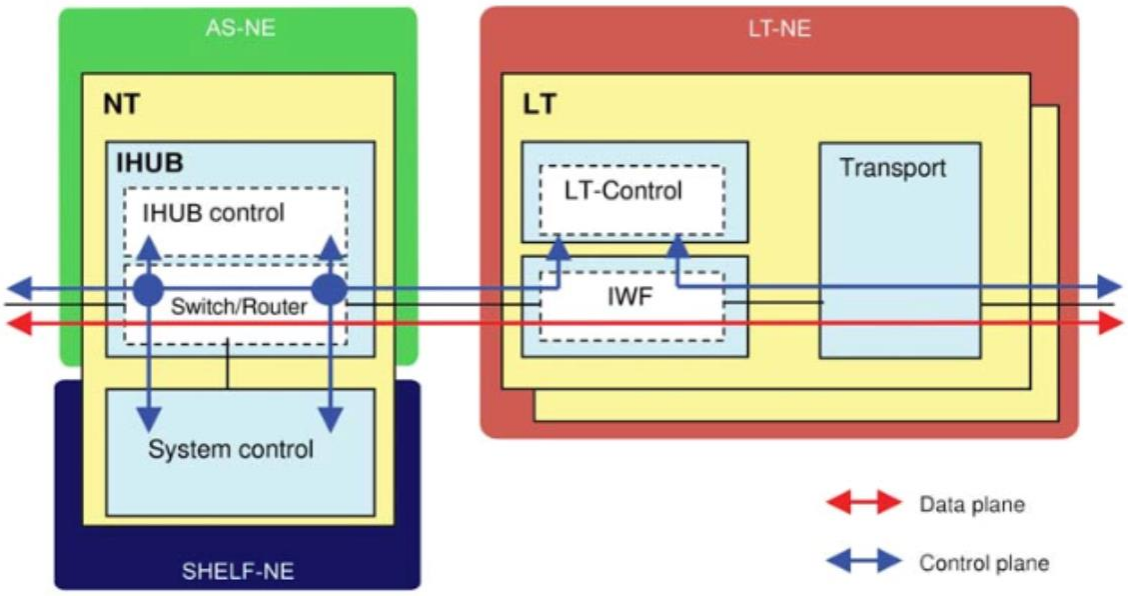
©2026 atsec information security AB

6 Architectural Information

The TOE is software only and consists of several standalone Network Elements (NE). These NEs are:

- a shelf Network Element (SHELF-NE) providing common equipment, software, alarm and log management.
- an Aggregation Switch (AS) of the IHUB Network Element (AS-NE) providing the switching and routing functionalities.
- multiple (O)LT Network Elements (LT-NE) providing xPON or P2P transport and forwarding functionality.

The figure below shows the high-level functional architecture of the main functional capabilities (from the viewpoint of its forwarding capabilities) and the mapping to the NE implementation of the TOE.



The NT board consists of an IHUB subsystem and a System Control subsystem.

- The IHUB subsystem consists of a switch/router device and IHUB control software (SW).
- The System Control subsystem implements the management plane of the system (both the NT board and the LT boards) and part of the control plane (subscriber management in particular).

LT boards typically have an InterWorking Function (IWF), a Transport subsystem and an LT-Control subsystem.

- The transport subsystem terminates the physical layer of the subscriber interfaces. It varies with the type of access technology used (Ethernet, PON).
- The IWF processes the packets in the fast path. It is capable of handling frames at L2 and L3, including sophisticated filtering and traffic management, all at the line rate of the transport medium.
- The LT-Control subsystem takes care of the slow path control plane and internal Operations and Maintenance applications.

Every instance of these NEs (LT-NE, AS-NE and SHELF-NE) has its dedicated management connections. Each Network Element (NE) is managed through protocols listed in the figure below. Small nodes are modelled as one NE. Larger nodes, such as Lightspan Access Node MF are modelled as multiple NE.

7 Supplementary Cybersecurity Information

The supplementary cybersecurity information, as defined in article 55 of [CSA], can be found on the following website(s):

Accessible information	Link
Reporting and publishing of vulnerabilities	https://www.nokia.com/we-are-nokia/security/products/cvd/
Guidance documentation	https://www.nokia.com/support/
Support duration	https://partners.nokia.com/English/

7.1 Documentation

The following documentation is provided with the TOE:

Guidance documentation	Identification/Reference
Lightspan Security Hardening guide	3JL-43000-ACAA-RJZZA
Customer Release Note	3TJ-00170-MAAA-FMZZB
Lightspan Access Node MF Release 25.12 System Description	3HH-13800-IAAA-TQZZA 22
Software package guide for 25.12	3HH-14266-AAAA-RJZZA 32
User Safety and Installation Manual for MF-2	3HH-90465-AAAA-RJZZA 21
Customer Documentation Package (package containing all the provided OAM Manuals): • Lightspan MF-2 Reference Configurations • Lightspan MF-2/LMNT-B OAM Manual • Lightspan MF-2/LMNT-B IHUB OAM Manual • Lightspan MF-2/LMNT-B Alarms • Lightspan MF-2/LMNT-B IHUB Alarms • LMNT-B eCLI Command Guide	3HH-92611-FAAA

©2026 atsec information security AB

8 ICT Product Evaluation

8.1 Assurance Components

The assurance components used for the evaluation of the TOE are the ones included in EAL3, augmented by ALC_FLR.2, as defined in [CC] and [CEM]. See chapter 9 for a full summary of all components included in the package.

8.2 State-of-the-Art Documents and Evaluation Criteria

No specific State-of-the-Art document was used in this evaluation.

No further Evaluation Criteria applicable.

No Protection Profile was applied during this evaluation.

8.3 Evaluated Configuration

In order to make the TOE securely managed, the operator must make sure that:

- A dedicated management access model is applied.
- The secure variants of the management interfaces are used:
  - NETCONF over SSH or TLS
  - CLI over SSH
  - Syslog over TLS
- The external log server should be the primary means of archiving audit records.
- A secure administrator authentication method is used. Refer to 'authentication' section in the OAM manuals.
- The only CLI that the administrators are using is the embedded YANG eCLI.
- Unused management interfaces are closed.
- All unused network service ports are closed.
- The debug port for troubleshooting is closed.
- The access control lists to limit access to the management IP address are configured.
- The default user accounts are managed.
- The default user passwords are changed.
- The strong encryption algorithms, key exchange algorithms and authentication algorithms are used.
- The 'system lockout' is configured to prevent brute force attacks.
- The 'idle timeout' is configured.
- The device Certificates are managed.
- The software download verification (verifying the authenticity of SW downloaded explicitly) is done during the software upgrade or migration process.

©2026 atsec information security AB

8.4 Developer Testing

The evaluators examined the testing conducted by the developer (coverage and functional testing) to ensure that the developers have fulfilled their responsibilities and covered all requirements. The depth of the developer testing reached down to the platform of the Lightspan OS and its mechanics.

The evaluator examined that the developer test cases covered all TSFIs and SFRs.

8.5 Evaluator Testing

For the independent testing, the evaluator repeated a sample of the tests conducted by the developer.

The evaluator also repeated a sample of the testing done by the developer. The focus of these tests was on the TSFIs present at the boundary of the TOE.

The ordering of independent tests was done in a way where tests with configurations were done early (e.g. SSH and Syslog over TLS) to verify that the state of the TOE and these configurations are maintained. The independent testing focused on coverage, with test cases covering all TSFI to some capacity. The testing also covered all subsystems present in the TOE.

All evaluator testing was conducted remotely from the premises of the ITSEF, with additional steps added to verify the testing environment being made in each session.

8.6 Penetration Testing

A public search for vulnerabilities was conducted according to a compiled list of terms related to the TOE and the environment used by the TOE.

The penetration testing efforts focused on finding and identifying the possible attack surfaces available, and in which way these surfaces could potentially be exploited. The VLAN was the primary surface when devising hypothetical attacks. The efforts also included work inside the VLAN in which the TOE will reside, which included port scans against the TOE interfaces that are accessible to a potential attacker residing in the VLAN. This included all IPv4 and IPv6 TCP and UDP ports of the TOE.

All penetration testing was conducted on the same setup as the independent testing.

©2026 atsec information security AB

9 Results of the Evaluation

9.1 Summary

Development		Result
Security Architecture	ADV_ARC.1	Pass
Functional specification	ADV_FSP.3	Pass
TOE design	ADV_TDS.2	Pass
Guidance documents		
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life-cycle support		
CM capabilities	ALC_CMC.3	Pass
CM scope	ALC_CMS.3	Pass
Delivery	ALC_DEL.1	Pass
Developer environment security	ALC_DVS.1	Pass
Development life-cycle definition	ALC_LCD.1	Pass
Flaw remediation	ALC_FLR.2	Pass
ST evaluation		
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
Security requirements	ASE_REQ.2	Pass
TOE summary specification	ASE_TSS.1	Pass
Tests		
Coverage	ATE_COV.2	Pass
Depth	ATE_DPT.1	Pass
Functional tests	ATE_FUN.1	Pass
Independent testing	ATE_IND.2	Pass

©2026 atsec information security AB

Vulnerability assessment		
Vulnerability analysis	AVA_VAN.2	Pass

9.2 Result

As defined in chapter 8.1, the evaluation was based on the EAL3 package augmented with ALC_FLR.2. This corresponds to a certificate on "Substantial" as defined in [EUCC].

The [ST] did not claim conformance to any PP.

Based on the above, the evaluation results from the ITSEF concluded that Nokia Lightspan Access Node MF-2 version 25.12 **is Part 2 extended and Part 3 conformant to the [CC].**

©2026 atsec information security AB

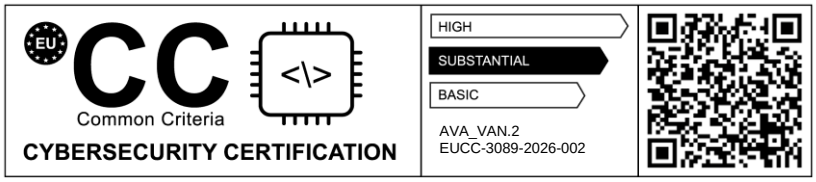
10 Certificate Information

A certificate has been issued following the conclusion of the evaluation.

Unique identifier for certificate: **EUCC-3089-2026-002**

Initial certificate issued: **2026-09-10**

Valid for: **5 years**



11 Comments and Recommendations

None.

12 Reference to the Security Target

The Nokia Lightspan Access Node MF-2 Security Target [ST] is provided as a separate document alongside this Certification Report.

13 Glossary

If applicable, this section is used to increase the readability of the report by providing definitions of acronyms or terms of which the meanings may not be readily apparent.

TOE	Target of Evaluation
ITSEF	IT Security Evaluation Facility
FMV	The Swedish Defence Material Administration
Swedac	The Swedish National Accreditation Body

©2026 atsec information security AB

14 Bibliography

[CC] Common Criteria for Information Technology Security Evaluation, CC:2022, revision 1, November 2022 — Parts 1 – 5

[CEM] Common Methodology for Information Technology Security Evaluation, CEM:2022, revision 1, November 2022 — Evaluation methodology

[ETR] Final Evaluation Technical Report, atsec information security AB, version 3.0, 2026-09-09

[ST] Nokia LightSpan Access Node MF Common Criteria Security Target, Nokia Solutions and Networks Oy, version 0.96, 2026-08-27

[SHG] Lightspan Security Hardening Guide Release 25.12, Nokia Solutions and Networks Oy, 2026-07-16

[PLC] Product Life Cycle Support, Nokia Solutions and Networks Oy, document ID 3HH-03851-0080-DFZZA

[CRN] Lightspan Access Node MF Customer Release Notes 25.12, Nokia Solutions and Networks Oy, 2025-12

[USI] User, Safety and Installation Manual for MF-2, Nokia Solutions and Networks Oy, Version 19, 2025-06

[SPG] Lightspan Access Node MF Software Package Guide, Nokia Solutions and Networks Oy, Version 32, 2025-12

[REC] Lightspan MF-2 Reference Configurations, Nokia Solutions and Networks Oy

[OAM] Lightspan MF-2 LMNT-B OAM Manual, Nokia Solutions and Networks Oy

[IOM] Lightspan MF-2 LMNT-B IHUB OAM Manual, Nokia Solutions and Networks Oy

[LMA] Lightspan MF-2 LMNT-B Alarms, Nokia Solutions and Networks Oy

[LIM] Lightspan MF-2 LMNT-B IHUB Manual, Nokia Solutions and Networks Oy

[EUCC] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024, amended by Commission Implementing Regulation (EU) 2024/3144 of 18 December 2024 and Commission Implementing Regulation (EU) 2025/2462 of 8 December 2025

[CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019

©2026 atsec information security AB