



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

Certification Report - Huawei OptiX OSN 1800 & OptiXtrans E6600 & DC908

Certification ID: EUCC-3089-2026-003

Certification Body ID: 3089

Version: 1.0

Author: Erik Ankarstad

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 9
2.2 Contact Information 9
2.2.1 Holder of Certificate 9
2.2.2 Certification Body 9
3 Security Policies 10
3.1 Authentication 10
3.2 Authorization 10
3.3 Auditing 10
3.4 Communication Security 10
3.5 Traffic Flow Control 10
3.6 Security Management 11
3.7 Cryptographic Functions 11
4 Vulnerability Handling and Assurance Continuity 12
4.1 Assurance Continuity 12
4.2 Patch Management 12
5 Assumptions and Clarification of Scope 13
5.1 Usage Assumptions 13
5.2 Environment Assumptions 13
5.3 Threats 14
5.4 Organisational Security Policies (OSP) 15
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 Document and Evaluation Criteria 18
8.3 Evaluated Configuration 18
8.4 Developer Testing 18
8.5 Evaluator Testing 18
8.6 Penetration Testing 18
9 Results of the Evaluation 20
9.1 Summary 20
9.2 Result 21
10 Certificate Information 22
11 Comments and Recommendations 23
12 Reference to the Security Target 24

©2026 atsec information security AB

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 Huawei OptiX OSN 1800 & OptiXTrans E6600 & DC908 management component software version V100R024C10SPC100 patch SPH105T.

The developer of the TOE is Huawei Technologies Co., Ltd.

The OSN Series device is transmission equipment and targets specific layers in the network. It is generally deployed in the upstream of wired broadband and mobile carrier facilities, which consists of software and hardware.

The OptiX OSN 1800 & OptiXtrans E6600 & DC908 is targeted for use at the edge/access layer. It can work with OptiX OSN 9800 to form a complete OTN-based end-to-end network for unified network management.

OptiX OSN 1800 and OptiXtrans E6600 are two different commercial brands for different customers. OptiX OSN 1800 is used by both carriers and enterprise networks, and OptiXtrans E6600 is a new commercial brand for enterprise networks.

The OptiX OSN 1800 series (V Pro/II TP/II Pro) are designed for the edge layers and it is generally deployed in the upstream of wired broadband and mobile carrier facilities. Services such as the broadband, SDH, and Ethernet services are processed at the edge access layer and then sent to the convergence node on the edge transport network. In this manner, it works with the OSN 9800/1800 to build a complete E2E WDM/OTN backbone transmission solution, achieving transparent and ultra-large capacity transmission.

The E6600 series (E6608/E6608T/E6616) and OptiXtrans DC908 are an intelligent all-optical transmission platform designed for enterprises. It can be widely used in industries such as electric power and transportation that are crucial to national economy and people's livelihood, guaranteeing that a large amount of production data is securely and reliably transmitted on the edge transport network in major cities.

The TOE is software only and consists of the respective software files for each hardware model it runs on, along with user documentation. The physical scope of the TOE is:

Type	Delivery Item	Version
Software	Software file, software signature file, patch file and patch signature file for hardware models: • OptiX OSN 1800 V Pro • OptiX OSN 1800 II Pro • OptiX OSN 1800 II TP • OptiXtrans E6616 • OptiXtrans E6608 • OptiXtrans E6608T • OptiXtrans DC908 • OptiXtrans DC908 Pro	V100R024C10SPC100
Product Guidance	Huawei Optix OSN 1800 & OptiXtrans E6600 & DC908 management component software V100R024C10SPC100 - AGD_OPE Huawei Optix OSN 1800 & OptiXtrans E6600&DC908 management component software V100R024C10SPC100 - AGD_PRE	0.6 0.10
Product Guidance	OptiXtrans DC908 Pro Product Documentation OptiXtrans DC908 Product Documentation	V100R024C10

©2026 atsec information security AB

	OSN 1800 V100R024C10 Product Documentation OptiXtrans E6600 V100R024C10 Product Documentation	
Product Guidance	OpitX OSN 1800 Series Security Configuration, Maintenance and Hardening Guide (NCE) OptiXtrans E6600 Security Configuration, Maintenance and Hardening Guide Huawei OptiXtrans DC908 Security Configuration, Maintenance and Hardening Manual (NCE) Huawei OptiXtrans DC908 Pro Security Configuration, Maintenance and Hardening Manual (NCE)	V100R024C10

Table 1: Physical scope

The evaluation was performed by atsec information security GmbH, located at Ismaninger Straße 19, 81675 Munich, Germany. atsec information security GmbH is accredited according to ISO/IEC 17025 by the German accreditation body DAkkS with accreditation number D-PL-21940-01-00.

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 four defined threats and to fulfil the two OSPs that have also been defined. See chapter 5 of this report for further information regarding the specific assumptions, threats, and OSPs.

The evaluation was completed in October, 2026. The evaluation was conducted in accordance with the Common Methodology for Information Technology Security Evaluation, CEM version 3.1, revision 5 [CEM], and corresponding Common Criteria for Information Technology Security Evaluation, CC version 3.1, revision 5, parts 1-3 [CC].

After reviewing the work of the evaluator, the Certification Body has issued the initial certificate for Huawei OptiX OSN 1800 & OptiXTrans E6600 & DC908 management component software version V100R024C10SPC100 on the 29th of October, 2026. The validity period is 5 years, and the certificate is therefore valid until 28th of October, 2031. The unique identifier of the certificate is **EUCC-3089-2026-003**.

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 Huawei OptiX OSN 1800 & OptiXTrans E6600 & DC908 management component software V100R024C10SPC100.

The following components make up the TOE.

Type	Reference	Version
Software	OptiX OSN 1800 V Pro: Software file: OptiX OSN 1800 V Pro_V100R024C10SPC100.zip Software Signature file: OptiX OSN 1800 V Pro_V100R024C10SPC100.zip.asc Patch file: OptiX OSN 1800 V Pro_V100R024C10SPH105T.zip Patch Signature file: OptiX OSN 1800 V Pro_V100R024C10SPH105T.zip.asc	V100R024C10SPC100
Software	OptiX OSN 1800 II Pro: Software file: OptiX OSN 1800 II Pro_V100R024C10SPC100.zip Software Signature file: OptiX OSN 1800 II Pro_V100R024C10SPC100.zip.asc Patch file: OptiX OSN 1800 II Pro_V100R024C10SPH105T.zip Patch Signature file: OptiX OSN 1800 II Pro_V100R024C10SPH105T.zip.asc	V100R024C10SPC100
Software	OptiX OSN 1800 II TP: Software file: OptiX OSN 1800 II TP_V100R024C10SPC100.zip Software Signature file: OptiX OSN 1800 II TP_V100R024C10SPC100.zip.asc Patch file: OptiX OSN 1800 II TP_V100R024C10SPH105T.zip Patch Signature file: OptiX OSN 1800 II TP_V100R024C10SPH105T.zip.asc	V100R024C10SPC100
Software	OptiXtrans E6616: Software file: OptiXtrans E6616_V100R024C10SPC100.zip Software Signature file: OptiXtrans E6616_V100R024C10SPC100.zip.asc Patch file:	V100R024C10SPC100

	OptiXtrans E6616_V100R024C10SPH105T.zip Patch Signature file: OptiXtrans E6616_V100R024C10SPH105T.zip.asc	
Software	OptiXtrans E6608: Software file: OptiXtrans E6608_V100R024C10SPC100.zip Software Signature file: OptiXtrans E6608_V100R024C10SPC100.zip.asc Patch file: OptiXtrans E6608_V100R024C10SPH105T.zip Patch Signature file: OptiXtrans E6608_V100R024C10SPH105T.zip.asc	V100R024C10SPC100
Software	OptiXtrans E6608T: Software file: OptiXtrans E6608T_V100R024C10SPC100.zip Software Signature file: OptiXtrans E6608T_V100R024C10SPC100.zip.asc Patch file: OptiXtrans E6608T_V100R024C10SPH105T.zip Patch Signature file: OptiXtrans E6608T_V100R024C10SPH105T.zip.asc	V100R024C10SPC100
Software	OptiXtrans DC908: Software file: OptiXtrans DC908_V100R024C10SPC100.zip Software Signature file: OptiXtrans DC908_V100R024C10SPC100.zip.asc Patch file: OptiXtrans DC908_V100R024C10SPH105T.zip Patch Signature file: OptiXtrans DC908_V100R024C10SPH105T.zip.asc	V100R024C10SPC100
Software	OptiXtrans DC908 Pro: Software file: OptiXtrans DC908 Pro_V100R024C10SPC100.zip Software Signature file: OptiXtrans DC908 Pro_V100R024C10SPC100.zip.asc Patch file: OptiXtrans DC908 Pro_V100R024C10SPH105T.zip Patch Signature file:	V100R024C10SPC100

©2026 atsec information security AB

	OptiXtrans DC908 Pro_V100R024C10SPH105T.zip.asc	

Table 2: Components

Along with the TOE, a set of guidance documents is provided. See chapter 7.1 for the full list of guidance documents.

See chapter 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 OptiX OSN 1800 V Pro/OptiX OSN 1800 II Pro/OptiX OSN 1800 II TP/OptiXtrans E6616/OptiXtrans E6608/OptiXtrans E6608T/OptiXtrans DC908/OptiXtrans DC908 Pro hardware. The TOE requires the following components to be used in the operating environment of the TOE, on systems other than those hosting the TOE:

- Local Maintenance Terminal (LMT) called iMaster NCE Web LCT
- Remote Maintenance Terminal (RMT) called iMaster NCE-T
- SFTP server

Additionally, the following components may be used in the operational environment:

- RADIUS server
- Syslog server
- NTP server

2.2 Contact Information

2.2.1 Holder of Certificate

Developer Name	Huawei Technologies Co., Ltd
Address	Bantian, Longgang District Shenzhen 518129 People's Republic of China
Contact	support@huawei.com
Website link for Supplementary Cybersecurity Information	https://support.huawei.com/enterprise/en/doc/EDOC1100605335

2.2.2 Certification Body

Name	atsec information security AB
Address	Svärdvägen 23 182 33 Danderyd Sweden
Contact	cb@atsec.com
ITSEF	atsec information security GmbH
NCCA	Swedish Defence Material Administration (FMV)

©2026 atsec information security AB

3 Security Policies

3.1 Authentication

All users that are connected must be authenticated and then they can operate the TOE. The TOE provides a local authentication mode, or can optionally enforce authentication decisions obtained from a Radius server in the IT environment.

In local authentication mode, accounts and passwords are saved on the local equipment and authenticated using the local account and password by the local equipment during login. In RADIUS authentication mode, accounts and passwords are saved on the RADIUS server and authenticated by the RADIUS server. During login, the accounts and passwords are forwarded to the RADIUS server, using the RADIUS protocol and the RADIUS server checks the validity of accounts and passwords.

User authentication is always enforced for RMT/LMT. The use of TLS connection is always required for accessing the TOE via RMT/LMT.

3.2 Authorization

The TOE controls access by the group-based authorization framework with predefined role groups for management. Four hierarchical access groups are offered and can be assigned to individual user accounts. Only authenticated users can execute operation of the TOE. Only one user group level can be assigned to a user account. So, the user group level of a user is unambiguous at any time.

3.3 Auditing

Logs record routine maintenance events of the TOE. Administrators can find security vulnerabilities and risks by checking logs. Considering security, the TOE provides security logs and operation logs.

Security logs record operation events related to account management, such as modification of passwords and addition of accounts. Operation logs record events related to system configurations, such as modification of equipment IP addresses and addition of services.

The TOE provides a Syslog solution to resolve the problem of limited equipment storage space. Both security logs and operation logs can be saved on an external Syslog server.

3.4 Communication Security

The TOE provides communication security by implementing the TLS/DTLS protocol and the SFTP protocol for different use cases.

For the secure communication between the TOE and the RMT/LMT/Syslog server the TLS protocol is used. TLS version 1.2 and 1.3 are implemented. TLS certificates are required for establishing TLS encryption channels. The TLS certificates are managed and issued by the user of the TOE (mainly Internet Service Providers ('carriers')). The TOE acts as server during the TLS communication established between the TOE and RMT/LMT, while it acts as client during the TLS communication with the Syslog server.

The TOE provides an SFTP client for secure file downloading and uploading. Users can use the SFTP client for fault collection, log uploading, and uploading and downloading of a file and a database etc. In this application, the TOE serves as a client and the SFTP server is deployed outside the equipment network and is provided by the carrier.

3.5 Traffic Flow Control

For administration of the TOE, network packages have to be sent to the TOE from the management network. The TOE provides Access Control List (ACL) for filtering incoming information flows to management interfaces. An Administrator can set deny IP addresses and ports, to limit data from specific IP addresses and to filter data from specific communication ports. The ACL function protects equipment from network attacks by controlling data of access requests from unauthorized IP addresses and ports. The Administrator can create, delete, and modify ACL rules in Table 1-4. Packet flows matching a deny rule in the ACL are dropped. If no rule is specified for an incoming packet, it is accepted by default.

3.6 Security Management

Security functionality management include not only authentication, access level, but also managing security related data consisting of configuration profile and runtime parameters. According to security functionality management, customized security is provided.

The functions mainly include:

- Management of user accounts and user attributes, including user credentials.
- Management of authentication failure policy
- Access control management, including the association of users and corresponding privileged functionalities.
- Enabling/disabling trusted channels for local and remote access to the TOE's management interfaces
- Management of ACLs and ACL attributes and parameters like IP addresses or address ranges
- Configuration of network addresses for services used by the TOE, like NTP, Syslog, RADIUS, SFTP
- Management of the TOE's time

3.7 Cryptographic Functions

The TOE does not offer cryptographic services, but uses cryptographic mechanisms in the implementation of its communication security functions (TLS, SFTP) and I&A functions (certificates, SFTP public key authentication).

©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:

- Huawei OSN Series management component software V100R024C10SPC100 – ALC_FLR, 2026-06-09, version 0.6

4.1 Assurance Continuity

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

4.2 Patch Management Process

A Patch Management in accordance with [EUCC] annex IV.4 is not applicable to this certification.

©2026 atsec information security AB

5 Assumptions and Clarification of Scope

The [ST] contains eight assumptions and four 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.NoEvil	It is assumed that personnel working as authorized users shall be carefully selected for trustworthiness and trained for proper operation of the TOE. These users are assumed being administration professionals, work not careless or willfully negligent or hostile, and will follow and abide the TOE documentation.
A.Device	It is assumed that the underlying hardware of OSN Series, which is outside the scope of the TOE, as well as the non-TOE software, work correctly and do not tamper with the TOE in any manner.

5.2 Environment Assumptions

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

Assumption	Description
A.TLSKeyandCertificate	It is assumed that the asymmetric keys for TLS end point authentication are generated in a secure way and are of good quality, i.e. meeting relevant standards and providing sufficient security strength. The corresponding certificates are obtained from trusted certification authorities by secure means and the certificates are of good quality, i.e. the cryptographic mechanisms and parameters used to sign the certificate meeting relevant standards and providing sufficient security strength. It is also assumed that Administrators validate the complete certificate chain and examine the quality of the certificates before importing them. Especially the Administrators check the hash algorithm used to sign the certificate and do not import certificates signed with weak hashing algorithms. The private keys are imported into the TOE in a secure way.
A.PhysicalProtection	It is assumed that the TOE and its operational environment (i.e. the complete system including the device hardware and attached peripherals) are protected against unauthorized physical access. It is assumed that only users with explicit approval by the Administrator(s) are authorized to physically access the TOE and its operational environment. This assumption includes the RADIUS server and NTP server together with all related communication lines are operated in the same physically secured environment as the TOE. For LMT, RMT, Syslog server and SFTP server, this assumption only includes the device itself.
A.NetworkElements	It is assumed that the operational environment provides securely and correctly working network devices as resources that the TOE needs to cooperate with. This applies e.g. to the LMTs and RMTs used for TOE management, Syslog servers, SFTP servers and Radius servers for

©2026 atsec information security AB

	obtaining authentication and authorization decisions. NTP servers for synchronizing time to the TOE.
A.NetworkSegregation	It is assumed that the operational environment provides segregation of networks by deploying the management interface in TOE into an independent local network.
A.RNG	It is assumed that the TPM, which provides the seed to the RNG, is reliable and therefore provides a seed value of sufficient entropy.
A.Time	It is assumed that the external clock provided by the NTP server is reliable.

5.3 Threats

The [ST] outlines four threats to the TOE.

Threat	Description
T.UnwantedManagementTraffic	The traffic here only refers to the traffic on management interfaces, that means, the Unwanted Network Traffic threat only exists on the management plane. The Unwanted network traffic may originate from an attacker and result in an overload of the management interfaces, which may cause a failure of the TOE to respond to system control and normal management operations. As a consequence, the TOE might be unable to provide some of the TSF while under attack and in particular security management functionality to update configuration data for the TOE. Subsequently, backup of audit information before local storage space is exceeded and old audit information is overwritten by new audit events could be affected. Therefore, Audit data and Configuration data for the TOE are assets that could be affected by this threat, too.
T.UnauthenticatedAccess	An unauthenticated person may attempt to bypass the security of the TOE so as to access and use security functions and/or non-security functions provided by the TOE. This could affect all assets.
T.UnauthorizedAccess	A user with restricted action and information access authorization gains access to unauthorized commands or information. This threat also includes data leakage to non-intended person or device. This could affect all assets.
T.Intercept	An attacker is able to intercept, modify and re-use management information assets that are exchanged between the TOE and RMT/LMT and between the TOE and the SFTP server. This comprises Authentication data (in particular authentication data of users), Crypto data (regarding this threat mainly data related to session keys used for secure communication), and Configuration Data for the TOE. In addition, an attacker is able to intercept and modify audit data that is transmitted to the external Syslog server. All these assets could be affected by this threat.

The threats, as outlined in the [ST], are 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.

©2026 atsec information security AB

5.4 Organisational Security Policies (OSP)

The [ST] outlines two Organisational Security Policies (OSP):

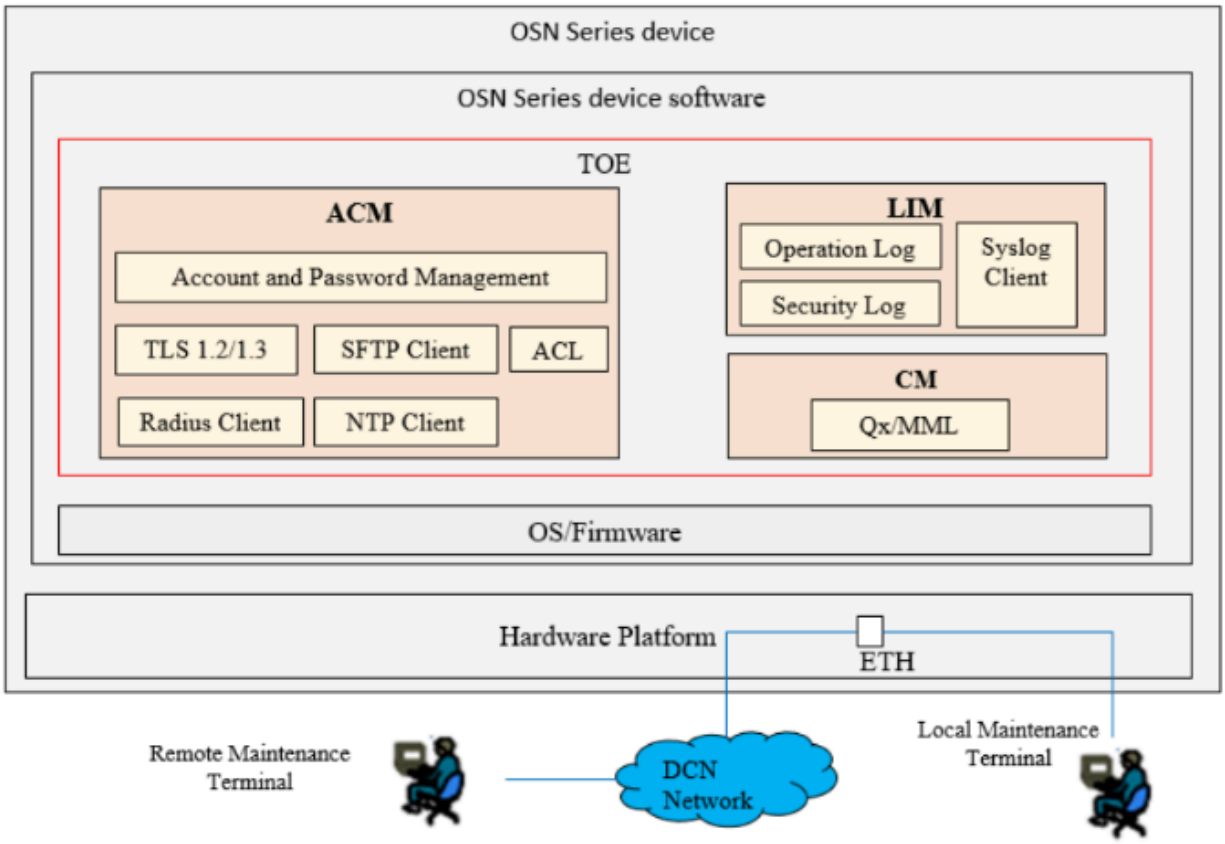
OSP	Description
OSP.Accountability	The users of the TOE shall be held accountable for their security-relevant actions within the TOE.
OSP.PasswordHash	User passwords shall be hashed in a secure way before being stored in the local storage of the TOE.

©2026 atsec information security AB

6 Architectural Information

The TOE is software only running on dedicated OSN series hardware. The TOE contains three subsystems:

- ACM: Access and Control Management Subsystem
- CM: Configuration Management Subsystem
- LIM: Log Information Management Subsystem



The ACM subsystem:

- Manages external access, for example, access by means of SFTP, RADIUS, SYSLOG, NTP, ACL and TLS
- Provides authentication and authorization functions
- Provides Command communication with user

The CM subsystem:

- Manages and executes the configuration commands of all the subsystems.
- Parses and executes QX and MML commands
- Saves, restarts and recovers configuration information through configuration management component

The LIM subsystem:

- Receives log information from other subsystems
- Exports logs in the specified format to log hosts
- Manages all logs

©2026 atsec information security AB

7 Supplementary Cybersecurity Information

Information	Website
Documentation and TOE information	https://support.huawei.com/enterprise/en/doc/EDOC1100605035
Vulnerability reporting and publishing	https://www.huawei.com/en/psirt/report-vulnerabilities
Support lifecycle	https://www.huawei.com/en/declarations/lifecycle-management-letter

7.1 Documentation

Guidance Documentation	Version
Huawei Optix OSN 1800 & OptiXtrans E6600 & DC908 management component software V100R024C10SPC100 - AGD_OPE	0.6
Huawei Optix OSN 1800 & OptiXtrans E6600&DC908 management component software V100R024C10SPC100 - AGD_PRE	0.10
OptiXtrans DC908 Pro Product Documentation OptiXtrans DC908 Product Documentation OSN 1800 V100R024C10 Product Documentation OptiXtrans E6600 V100R024C10 Product Documentation	V100R024C10
OpitX OSN 1800 Series Security Configuration, Maintenance and Hardening Guide (NCE) OptiXtrans E6600 Security Configuration, Maintenance and Hardening Guide Huawei OptiXtrans DC908 Security Configuration, Maintenance and Hardening Manual (NCE) Huawei OptiXtrans DC908 Pro Security Configuration, Maintenance and Hardening Manual (NCE)	V100R024C10

©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 Document 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

For testing the OSN 1800 II Pro model was used.

The evaluated configuration is defined in [PRE], a document which is delivered alongside the TOE.

The environment for the TOE comprises the following components:

- The LMT (Local Maintenance Terminal)/RMT (Remote Maintenance Terminal) accesses the TOE via the ethernet interfaces, and the communication is protected by TLS.
- The OSN Series hardware and OSN series non-TOE software are part of the operational environment.
- A Radius server, a Syslog server, an NTP server, and an SFTP (FTP over SSH) server as part of the operational environment.

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. Specific, manual tests were designed for the [CC], while a suite of automatic tests existed as part of the release process.

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 repeated tests covered all TSFIs to some capacity.

The evaluator chose test cases based on the typical use cases for the security functions of the TOE, functionality marked as optional in the guidance and parts of the guidance which were first unclear to the evaluator while configuring the TOE. Enforcement of TLS version and TLS cipher suite was tested, as well as patch installation and NTP sync to the NTP server.

All evaluator testing was conducted at the premises of the ITSEF.

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.

As with the general evaluator testing, the penetration tests were chosen based on the typical use cases for the security functions of the TOE, functionality marked as optional in the guidance and parts of the guidance which were first unclear to the evaluator while configuring the TOE. A Man-in-the-Middle attack was conducted to verify that iMaster and the TOE verify their certificates of the TLS channel at the correct

port, and that the TOE validates the DTLS certificate of the RADIUS server. A port scan was also conducted to verify that only known TCP and UDP ports were open.

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
Vulnerability assessment		
Vulnerability analysis	AVA_VAN.2	Pass

©2026 atsec information security AB

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 Huawei OptiX OSN 1800 & OptiXTrans E6600 & DC908 management component software version V100R024C10SPC100 **is Part 2 extended and Part 3 conformant to the [CC].**

©2026 atsec information security AB

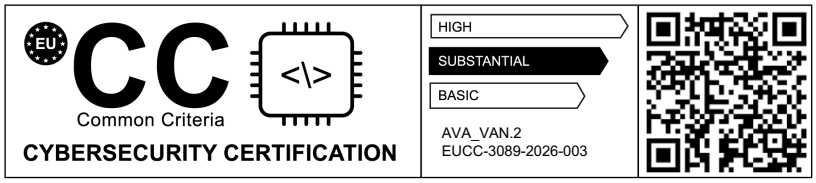
10 Certificate Information

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

Unique identifier for certificate: **EUCC-3089-2026-003**

Initial certificate issued: **2026-10-29**

Valid for: **5 years**



©2026 atsec information security AB

11 Comments and Recommendations

None.

12 Reference to the Security Target

The Huawei OptiX OSN 1800 & OptiXtrans E6600 & DC908 management component software V100R024C10SPC100 - ST [ST] is provided as a separate document alongside this Certification Report.

©2026 atsec information security AB

13 Glossary

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

©2026 atsec information security AB

14 Bibliography

[CC] Common Criteria for Information Technology Security Evaluation, CC version 3.1, revision 5, April 2017 — Parts 1 – 3

[CEM] Common Methodology for Information Technology Security Evaluation, CEM version 3.1, revision 5, April 2017 — Evaluation methodology

[ETR] Final Evaluation Technical Report, atsec information security GmbH, version 1.3, 2026-10-23

[ST] Huawei OptiX OSN 1800 & OptiXtrans E6600 & DC908 management component software V100R024C10SPC11 - ST, Huawei Technologies Co., Ltd, version 0.16, 2026-10-14

[OPE] Huawei OptiX OSN 1800 & OptiXtrans E6600 & DC908 management component software V100R024C10SPC100 - AGD_OPE, Huawei Technologies Co., Ltd, version 0.6, 2025-09-24

[PRE] Huawei OptiX OSN 1800 & OptiXTrans E6600 & DC908 management component software V100R024C10SPC100 - AGD_PRE, Huawei Technologies Co., Ltd, version 0.10, 2026-02-26

[PD] OptiX OSN 1800 V100R024C10 Product Documentation, Huawei Technologies Co., Ltd, 2025-03-31

[CMH] OptiX OSN 1800 Security Configuration, Maintenance and Hardening Guide (NCE), Huawei Technologies Co., Ltd, version 12, 2026-03-31

[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