Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1030-2018

for

Huawei OptiX OSN 1800 V V100R006C20 software management component

from

Huawei Technologies Co., Ltd.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1030-2018 (*)

Network Device

Huawei OptiX OSN 1800 V V100R006C20 software management component

from	Huawei Technologies Co., Ltd.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 4

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement

Bonn, 26 October 2018

For the Federal Office for Information Security

Bernd Kowalski
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG1 Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

2. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[1]
- BSI Certification and Approval Ordinance[2]
- BSI Schedule of Costs[3]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[2] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[3] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

3. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

3.1. European Recognition of CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4. For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

3.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized under CCRA-2014 for all assurance components selected.

[4] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

4. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Huawei OptiX OSN 1800 V V100R006C20 software management component has undergone the certification procedure at BSI.

The evaluation of the product Huawei OptiX OSN 1800 V V100R006C20 software management component was conducted by atsec information security GmbH. The evaluation was completed on 25 October 2018. atsec information security GmbH is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Huawei Technologies Co., Ltd.

The product was developed by: Huawei Technologies Co., Ltd.

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

5. Validity of the Certification Result

This Certification Report applies only to the version of the product as indicated. The confirmed assurance package is valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance components and assurance levels please refer to CC itself. Detailed references are listed in part C of this report.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-assessment or re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods would require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 26 October 2018 is valid until 25 October 2023. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[5] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

6. Publication

The product Huawei OptiX OSN 1800 V V100R006C20 software management component, has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[6] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[6] Huawei Technologies Co., Ltd.

Huawei Industrial Base
Bantian, Longgang
Shenzhen, 518129
People's Republic of China

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is Huawei OptiX OSN 1800 V V100R006C20 software management component. It is part of the overall product OptiX OSN 1800 V. The overall product is a transmission equipment and is mainly applicable to the access layer and the aggregation layer of the metropolitan area network. It is generally deployed in the upstream of wired broadband and mobile carrier facilities, and consists of software and hardware.

The non-TOE product hardware is composed of cabinet, chassis, power unit, and boards. The cabinet is used to install chassis and power units that supply power to the chassis. The chassis provides the board slot to insert boards.

The boards are the core unit of processing and management in transmission equipment, consisting of the SCC (System Control and Communication) unit and the service units including the OTN line board, the Optical layer board, the Packet board, and the TDM board.

The SCC (System Control and Communication) unit is the center of the system. It collaborates with the non-TOE EMS (Element Management System) in order to centralize control, manage all service units of the system and implement inter-equipment communication. The EMS manages OptiX equipment using a GUI interface (i.e., the user interface of Huawei's U2000 management software). The GUI interface complies with a special management protocol defined by Huawei exclusively for OptiX equipment.

The OptiX OSN 1800 V software deployed in the SCC unit and service units is responsible for the system management, control, and service transmission.

The TOE is part of the OptiX OSN 1800 V software and only runs on the SCC unit. It consists of the (UTS) component and the underlying OS for the System Control and Communication unit (TNZ5UXCMS). These components provide the core control and management services of the device.

The non-TOE software components of the whole OptiX OSN 1800 V software include the system and service attribute management, the service schedule and protect, the optical Layer protocol, service warnings and performance, and the service control and monitor.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
Authentication	The TOE can identify users based on unique IDs and enforce their authentication before granting them access to any TSF management interfaces.

TOE Security Functionality	Addressed issue
Authorization	The TOE enforces an access control.
Auditing	The TOE provides an audit trail consisting of operation logs and security logs.
Communication Security	The TOE provides communication security by implementing TLS version 1.1 and 1.2 in the role of the server and SFTP with SSHv2 in the role of the client.
Management Traffic Flow Control	The TOE uses ACL to deny unwanted network traffic on management interfaces and allow wanted network traffic on management interfaces.
Security Management	The TOE allows management of the equipment network by different users. The TOE can be configured to grant each user the access right to the equipment network resources that are required for user operations.
Time	The TOE provides its own clock and timestamps to correctly record logs in time sequence or other place wherever the time shall be used. The time information on the TOE can either be set by a user with sufficient access rights on the device or obtained from external NTP time sources.
Cryptographic functions	The TOE supports several Cryptographic functions that are required by security features as dependencies.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Huawei OptiX OSN 1800 V V100R006C20 software management component

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Software OptiX OSN 1800 V100R006C20SPC300 Software.zip SHA-256 checksum: 2acd6990d24786dc7b27b35e6111b3e97e7203b53a2a648af7fdf302bdb6f8bc	V100R006C20SPC300	Pre-installed on the OptiX OSN 1800 V device delivered in a sealed parcel and on CD
2	DOC	Software signature file OptiX OSN 1800 V100R006C20SPC300 Software.zip.asc	-	On CD which is included in the sealed parcel
3	DOC	Guidance OSN 1800 V & 1800 I II Compact V100R006C20 Deploying Your Network [8]	03	On CD which is included in the sealed parcel
4	DOC	Guidance CC Huawei Optix OSN 1800V Software V100R006C20 - AGD_OPE [9]	V0.5	On CD which is included in the sealed parcel
5	DOC	Guidance CC Huawei Optix OSN 1800V Software V100R006C20 - AGD_PRE_Production [10]	V0.4	On CD which is included in the sealed parcel
6	DOC	Guidance CC Huawei Optix OSN 1800V Software V100R006C20 - AGD_PRE_User [11]	V1.1	On CD which is included in the sealed parcel
7	DOC	Guidance CC Huawei Optix OSN 1800V Software V100R006C20 - Software Configuration and Reference [12]	V0.7	On CD which is included in the sealed parcel

Table 2: Deliverables of the TOE

Note that although the SW also comes on CD, the installation of SW from CD was not part of the evaluation. The TOE is already installed on the device when it is sent to the customer. Especially the configuration of the cryptographic parameters is already done and cannot be changed by the customer (except for the disabling of the TLS 1.0 and SSL 3.0 which has to be performed by the user).

The TOE SW was tested and is running on an SCC board with the hardware revision identifier TNZ5UXCMS.

Huawei installs the software on the OSN 1800 V device, packs the parcel including a CD with the TOE documentation, the software package and the signature file and positions anti-tamper tags on the parcel. This parcel is then sent to the customer via a trusted shipping company. The customer is accompanied by a Huawei technical support engineer when configuring the device and deploying the services. They first

- verify the integrity of the parcel,
- check the version of the already installed software,
- check the versions of the TOE documentation provided on CD.

If all the checks in the above list of bullet points are successfully passed, the device can be configured. After the configuration of the device and the deployment of the services the TOE is handed over to the customer.

The customer is informed by Huawei about the logistics company which will deliver the device to him. The customer has to check that the company which delivered the TOE matches the information the customer received in advance from Huawei. If it does not match, the customer shall not accept the parcel. Additionally, the customer has to check all anti-tamper tags on the cardboard box that contains the TOE. The customer shall check whether the anti-tamper tags are incomplete and whether they are damaged. The customer also has to check whether the anti-tamper tags are marked with VOID. If any of the anti-tamper tags shows any of the described signs of tampering, the customer shall reject the parcel.

The Huawei project supervisor / Huawei on-site technical support engineer works with the customer to unpack and inspect the delivered equipment. The deliverables are inspected against the Packing List and in case of damage or any other deviation the project supervisor fills in the Equipment Problem report and send it to the order management engineer of the local office of Huawei within three days. The customer and the Huawei technical support engineer install and configure the device and verify after power-on the version of the software against the stated version in this report and in the ST [6].

The TOE version can be obtained by performing the following command on the command prompt:

display version

The response will be:

"*Huawei Versatile Routing Platform Software VRP (R) software, Version 5.130 (Optix OSN 1800 V100R006C20).*"

The version information given in brackets reflects the TOE with its unique version number.

The TOE version can also be obtained by querying for the software version of the system control board on the EMS, here U2000. On the U2000, one has to choose Properties from the main menu selecting the desired network element and the software version of the OSN 1800 V system control board will be shown. The TOE reference which has to be shown is "V100R006C20SPC300".

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. You will find a summary in the ST [6] chapters 1.5.3.1 to 1.5.3.7.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. You will find the list of relevant topics in the ST [6], chapter 4.2.

5. Architectural Information

The TOE only consists of the unified transmission software (UTS), and the underlying OS, see red frame in Figure 1-5 of the ST [6] . The unified transmission software (UTS) and the underlying OS are the control and management core that runs on the SCC unit, which is responsible for managing and controlling the whole OptiX OSN 1800 V software, communication, and security features in OptiX OSN 1800 V. The TOE security functionalities are realized by three subsystems, namely Access Control Management (ACM), Configuration Management (CM), and Log Information Management (LIM), supported by the OS subsystem. The UTS platform running ACM, CM, and LIM is the major component responsible for most functionalities.

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

Developer testing:

The developer uses exclusively manual tests to test the TOE. As test environment setup the following material and tools were used by the developer:

- NE: Huawei OptiX OSN 1800 V in Version V100R006C20SPC300
- Switch: Ethernet Switch
- Two PCs: Host (OS of Windows 7)
- EMS: U2000 Unified Network Management System in Version V200R016C50SPC201
- MML test tool: Navigator 7.0
- Qx test tool: Impeller 1.9.2.9418
- Simulation of Syslog server: openssl-1.0.2n
- SFTP Server: Bitvise SSH Server 5.60
- RADIUS Server: FreeRadius3.0.16

Additionally, the general requirements for the configuration outlined in Preparative Procedures for Users [10] were used.

The developer's testing approach mostly concentrates on the verification of product functions that are expected by the typical user, a network administrator of a networking service provider or a large enterprise. This approach is evident by the tests with the developer's GUI, the U2000 user interface software, the test cases are executed manually. An automated testing framework does not exist.

The U2000 software makes use of the Qx protocol on its backend to the TOE, which is one of the TSFI. The developer also provided test cases for TLS and SFTP. Test cases for any of the other TSFI (MML, RADIUS, syslog, NTP) are not explicitly provided by the developer. Instead, implicit coverage of some of the TSFI other than the Qx protocol is given for cases where the U2000 interface controls the behaviour of the other TSFI (which is the case for functional aspects of NTP, RADIUS, syslog or SFTP).

The developer testing shows the absence of any test cases for the Qx protocol without any U2000 interaction and the absence of any test case for any of the other TSFI except TLS and SFTP as a limitation for the overall testing effort of the developer. Technically, the supplied test cases are free from situations where the configuration of the TOE would impose challenges for the individual test case, specifically with regards to preparation or clean-up of configurables, or where the ordering of test cases is of importance.

The developer has provided test cases for the following TSFI: Qx, SFTP/SSH, TLS, RADIUS, syslog. The developer does NOT provide test cases against the following TSFI: MML, NTP.

The limitation in the supplied tests was compensated by evaluator tests.

Evaluator Testing:

The evaluator has performed 19 of the developer's tests (of a total of 28 test cases), and additional four tests consisting of multiple variations in his independent tests. The evaluator's independent tests attempt to make precise observations about the TOE's behaviour as exposed by the U2000 interface in order to confirm possible limitations in the developer's testing approach, specifically the use of the U2000 software and its ability to display conditions of the TOE reliably and consistently, as well as the incompleteness in the coverage of the TSFI that are tested by the developer.

The configuration of the TOE to which the tests applies is compatible with the definitions given in the Security Target [6] section 3, more specifically the definition of threats and the assumptions (sections 3.3 and 3.4) as well as the objectives for the environment as stated in chapter 4.2. The developer tests are documented in such way that each test case contains descriptions about the necessary configuration parameters of the TOE that need to be set prerequisite to being able to conduct the respective test. The evaluator has maintained this type of self-sufficiency of the test cases in his own test plan.

The evaluator could successfully conduct the test cases and could confirm the developer's documented results.

Evaluator Penetration Testing:

The penetration testing was performed using the test environment of the evaluation lab. The configuration of the TOE being intended to be covered by the current evaluation was tested. The overall test result is that no deviations were found between the expected and the actual test results; moreover, no attack scenario with the attack potential Basic was actually successful.

The evaluator analyzed the developer design and guidance documentation and the Security Target in order to identify the attack surface of the TOE. The evaluator came to the conclusion that the attack surface consists of external network interfaces, i.e., data that is sent or received on these interfaces, and the two coexisting management interfaces (Qx and MML) with a similar functionality. The evaluator also used publicly documented vulnerabilities in the CVE database and used general search engines. The analysis of potential attack surfaces was performed according to the ISO/OSI layer model and knowledge of the design and architecture of the TOE.

The TOE and the TOE environment was configured according to [6] and the guidance documentation.

The evaluator performed TCP and UDP port scans of the TOE interfaces from the internal network to detect any potential attack surfaces. The evaluator also performed tests on TLS and SFTP/SSH. For the two management interfaces Qx and MML the evaluator performed concurrency tests and tested whether the interfaces behave in the same way.

The following list of SFRs were tested: FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, all FCS_* except FCS_CKM.4/*, FCS_COP.1/PBKDF2 and FCS_RNG.1, FDP_ACC.1, FDP_ACF.1, FDP_IFC.1, FIA_AFL.1, FIA_UAU.2, FIA_UAU.5, FIA_UID.2, FMT_SMR.1, FTA_TSE.1, FTP_ITC.1/TLS, and FTP_ITC.1/SFTP.

The remaining SFRs were analysed, but not penetration tested due to non-exploitability of the related attack scenarios in the TOE's operational environment also including an attacker with a Basic attack potential.

The overall test result is that no deviations were found between the expected and the actual test results. No attack scenario with the attack potential Basic was actually successful in the TOE's operational environment as defined in [6] provided that all measures required by the developer are applied.

8. Evaluated Configuration

This certification covers the following configurations of the TOE:

- For the management interface, authentication is always enabled. Authentication mode is Authentication, Authorization, Accounting ('AAA', i.e. username and password). Length of password is 16 characters.
- Service of FTP has to be disabled to use the TOE in the certified configuration
- SSL 3.0 and TLS 1.0 is disabled.
- The SSH server functionality is disabled.
- The gateway service functionality is disabled.
- The OSPF protocol is disabled.

The environment of the TOE consists of Local PCs and Remote PCs. Local PCs are used by administrators to connect to the TOE through interfaces on the SCC unit via a TLS channel or non-secure channel. Access will be performed using a command line terminal. Remote PCs are used by administrators to connect to the TOE using a TLS channel. Since the TOE is part of the OptiX OSN 1800 V device, it can only operate as part of the device. Hence all non-TOE parts of the device are also required. The TOE also needs in its environment an EMS (Element Management System), a Syslog server and an SFTP Server. A RADIUS server is optional and may be used instead of local authentication.

The non-TOE SW components include system and service attribute management, service schedule and protect, optical Layer protocol, service warning and performance, and service control and monitor.

For details please see chapters 1.5.1 and 1.5.2 of the ST [6].

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But cryptographic functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

The following table gives an overview of the cryptographic functionalities inside the TOE to enforce the security policy and outlines its rating from cryptographic point of view. Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context) only.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation [13]	Key Size in Bits	Security Level above 100 Bits	Comments
Cryptographic Functions for TLS:						
1	Authentication (Server)	X.509 certificates	RFC4346 (TLS1.1), RFC5246 (TLS1.2)	-	-	-
2	Authentication (Server)	RSA signature generation (RSASSA-PKCS1-v1_5) using SHA-256	RFC3447 (PKCS#1 v2.1) RFC5246 (TLSv1.2) FIPS186-4, B.3 FIPS180-4 (SHA)	Modulus length: 2048 to 4096 bits	yes	Certificates with encryption and signing capability.
3	Authentication (Client)	Password-based on application layer (16 characters over an alphabet of 94 characters)		log_2(|alphabet| ^password length) ~104,8 bit	yes	
4	Key establishment: Key transport	RSA decryption (server) (RSAES-PKCS1-v1_5) (TLS_RSA)	RFC3447 (PKCS #1 v2.1) SP800-56B (IFC key establishment)	min (asymmetric yes key strength, symetric key length)	yes	Server certificate is used for key exchange. Encrypted exchange of pre-master secret generated at client side.
5	Key establishment: Key agreement Ephemeral	TLS_DHE	RFC3526 (for the group diffie-hellman-group 14) RFC4346 (TLS 1.1) RFC5246 (TLS 1.2) SP800-56A (DH) PKCS3	diffie-hellman-group14	yes	This is the only group that is hard coded in the TOE.
6	Key derivation	PRF: HMAC with SHA-256, SHA-384 (default: prf_sha256 for TLSv1.2, also prf_sha384 possible	RFC2104 (HMAC) FIPS180-4 (SHA) RFC5246 (TLSv1.2)	variable	yes	
7	Key derivation	PRF: HMAC with MD5 and SHA-1 in combination (default: prf for TLS v1.1)	RFC2104, FIPS198-1 (HMAC) RFC1321 (MD5) FIPS180-3 (SHA) RFC4346 (TLS v1.1)	variable	no	
8	Confidentiality	AES in CBC mode (AES_128_CBC, AES_256_CBC)	FIPS197 (AES) SP800-38A (CBC)	|k|=128, 256	yes	Bulk data encryption / decryption (record layer)
9	Authenticated Encryption	AES in GCM mode (AES_128_GCM, AES_256_GCM)	FIPS197 (AES) SP800-38D (GCM) RFC5288 (AES GCM within TLS)	|k|=128, 256	yes	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation [13]	Key Size in Bits	Security Level above 100 Bits	Comments
10	Integrity and authenticity	HMAC with SHA-1 or SHA-256 (SHA), (SHA256)	RFC2104 (HMAC) FIPS180-3, FIPS180-4 (SHA)	160 (SHA-1) 256 (SHA-256)	yes	Message authentication code (record layer)
11	Trusted Channel	FTP_ITC.1/TLS in ST [6], Sec. 6.2.8.1	cf. all lines above	see above	yes/no	Depending on the sec. level of the used mechanisms above.
Cryptographic Functions for SSH/SFTP Security:						
1	Authentication	RSA signature generation & verification RSASSA-PKCS1-v1_5 using SHA-256 (ssh-rsa)	RFC3447 (PKCS#1 v2.1) RFC4253 (SSH-TRANS) Sec. 6.6 for host authentication RFC4252, Sec. 7 (SSH-USERAUTH) for user authentication method: "publickey"	Modulus length: 2048 to 4096	yes	Pubkeys are exchanged trustworthy out of band. Authenticity is not part of the TOE. (no certificates used)
2	Authentication	UserID & password	RFC4252, Sec. 8 (SSH-USERAUTH) for user authentication method: “password”	Guess success prob. <= 2^(-20)	yes/no (depending on server policy)	The client authenticates either with UserID & password or by cryptographic means as shown in #1. Password-based authentication is set by default.
3	Key establishment: Key agreement	DH with diffe-hellman -group14-sha1	RFC4253 (SSH-TRANS) supported by RFC3526 (DH groups IKE) FIPS180-3 (SHA-1)	plength=2048	yes	Hard coded in the TOE code.
4	Confidentiality	AES in CTR mode (aes128-ctr, aes192-ctr, aes256-ctr)	FIPS197 (AES), SP800-38A (CTR), RFC4253 (SSH using AES with CTR mode)	|k|= 128, 192, 256	yes	Binary packet protocol: encryption
5	Integrity and authenticity	HMAC-SHA-1 (hmac-sha1, hmac-sha1-96)	FIPS180-3 (SHA), RFC2104, FIPS198-1 (HMAC), RFC4251 / RFC4253 (SSH general / detailed HMAC support)	|k|=160	yes	Binary packet protocol: message authentication truncation: output length 96 bit
6	Key generation	RSA key generation using CRT with key size: 2048 to 4096 bits 5 rounds of Miller-Rabin	FIPS186-4, Sec. 5.1, B.3.3 and C.3.1 Miller Rabin probabilistic primality test.	n/a	n/a	Key generation FCS_CKM.1/ RSA using FCS_RNG.1

No.	Purpose	Cryptographic Mechanism	Standard of Implementation [13]	Key Size in Bits	Security Level above 100 Bits	Comments
7	Trusted Path	FTP_ITC.1/SFTP in ST [6], Sec. 6.2.8.2 for SSH/SFTP	See above	n/a	yes/no (depending on server policy)	
Cryptographic Function for password encryption:						
1	Authentication	PBKDF2 (HMAC-SHA256, 10000 iterations)	RFC2898	n/a	n/a	

Table 3: TOE cryptographic functionality

Note: The Standards of Implementation are referenced in [13].

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process, too.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a finalized version of the working version of the Security Target [6] that was used for the performed evaluation. Their contents are identical, only some formattings, version histories, and document classifications differ.

12. Definitions

12.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CM	Configuration Management
cPP	Collaborative Protection Profile
CTR	Counter Mode
CVE	Common Vulnerabilities and Exposures
DHE	Diffie Hellman Ephemeral
EAL	Evaluation Assurance Level
EMS	Element Management System
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GCM	Galois/Counter Mode
GUI	Graphical User Interface
HMAC	Hash Message Authentication Code
ISO	International Organization for Standardization
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LIM	Log Information Management
MML	Man MachineLanguage
NTP	Network Time Protocol
OSI	Open Systems Interconnection
OSN	Optical Switch Node
OTN	Optical Transport Network
PBKDF2	Password-Based Key Derivation Function 2
PP	Protection Profile
PRF	PseudoRandom Function
Qx	A proprietary interface
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RSA	Rivest, Shamir und Adleman

SAR	Security Assurance Requirement
SCC	System Control and Communication)
SFP	Security Function Policy
SFR	Security Functional Requirement
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SP	Special Publication
SSL	Secure Socket Layer
ST	Security Target
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UDP	User Datagram Protocol
UTS	Unified Transmission Software

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 5, April 2017
Part 2: Security functional components, Revision 5, April 2017
Part 3: Security assurance components, Revision 5, April 2017
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[7] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-1030-2018, Security Target for Huawei OptiX OSN 1800 V V100R006C20 software management component, Version 1.53, Date 2018-10-10, Huawei Technologies Co., Ltd. (confidential working document) and Security Target Lite BSI-DSZ-CC-1030-2018, Security Target Lite for Huawei OptiX OSN 1800 V V100R006C20 software management component, Version 1.53, Date 2018-10-10, Huawei Technologies Co., Ltd. (finalized public document)

[7] Evaluation Technical Report for BSI-DSZ-CC-1030, OptiX OSN 1800 V Version V100R006C20, Version 3, Date 2018-10-24, atsec information security GmbH, (confidential document)

[8] Huawei OptiX OSN 1800 V Packet Enhanced &1800 I/II Compact Deploying your Network V100R006C20, Version 03, Date 2017-04-28, Huawei Technologies Co., Ltd.

[9] Huawei OptiX OSN 1800V software V100R006C20, Operational User Guidance, Version 0.5, Date 2018-09-10, Huawei Technologies Co., Ltd.

[10] Huawei OptiX OSN 1800V software V100R006C20, Preparative Procedures for Production, Version 0.4, Date 2018-03-28, Huawei Technologies Co., Ltd.

[11] Huawei OptiX OSN 1800V software V100R006C20 Preparative Procedures for Users, Version 1.1, Date 2018-09-10, Huawei Technologies Co., Ltd.

[12] Huawei OptiX OSN 1800 V Software Configuration and Reference, Version 0.7, Date 2018-09-10, Huawei Technologies Co., Ltd.

[7] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

[13] - **FIPS180-3**: FIPS PUB 180-3 Secure Hash Standard (SHS), Date 2008-10
- **FIPS180-4**: FIPS PUB 180-4 Secure Hash Standard (SHS), Date 2012-03
- **FIPS186-4**: FIPS PUB 186-4 Digital Signature Standard (DSS), Date 2013-07
- **FIPS197**: FIPS PUB 197 Advanced Encryption Standard (AES), Date November 2001
- **FIPS198-1**: FIPS PUB 198-1 The Keyed-Hash Message Authentication Code (HMAC), Date 2008-07
- **PKCS #3**: PKCS #3: Diffie-Hellman Key-Agreement Standard, Author(s) RSA Laboratories, Version 1.4, Date 1993-11
- **RFC1321**: The MD5 Message-Digest Algorithm, Date 1992-04
- **RFC2104**: HMAC: Keyed-Hashing for Message Authentication, Author(s) H. Krawczyk, M. Bellare, R. Canetti, Date 1997-02-01
- **RFC2898**: PKCS #5: Password-Based Cryptography Specification Version 2.0, Author(s) B. Kaliski, Date 2000-09-01
- **RFC3447**: Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Date 2003-02
- **RFC3526**: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), Author(s) T. Kivinen, M. Kojo, Date 2003-05-01
- **RFC4251**: The Secure Shell (SSH) Protocol Architecture, Author(s) T. Ylonen, C. Lonvick, Date 2006-01-01
- **RFC4252**: The Secure Shell (SSH) Authentication Protocol, Author(s) T. Ylonen, C. Lonvick, Date 2006-01
- **RFC4253**: The Secure Shell (SSH) Transport Layer Protocol, Author(s) T. Ylonen, C. Lonvick, Date 2006-01-01
- **RFC4346**: The Transport Layer Security (TLS) Protocol Version 1.1, Author(s) T. Dierks, E. Rescorla, Date 2006-04-01
- **RFC5246**: The Transport Layer Security (TLS) Protocol Version 1.2, Author(s) T. Dierks, E. Rescorla, Date 2008-08-01
- **RFC5288**: AES Galois Counter Mode (GCM) Cipher Suites for TLS, Author(s) J. Salowey, A. Choudhury, D. McGrew, Date 2008-08-01
- **SP800-38A**: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Date December 2001
- **SP800-38D**: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Date November 2007
- **SP800-56A**: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Version R2, Date May 2013
- **SP800-56B**: NIST Special Publication 800-56B Rev. 1 - Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography, Version R1, Date September 2014

C. Excerpts from the Criteria

For the meaning of the assurance components and levels the following references to the Common Criteria can be followed:

- On conformance claim definitions and descriptions refer to CC part 1 chapter 10.5
- On the concept of assurance classes, families and components refer to CC Part 3 chapter 7.1
- On the concept and definition of pre-defined assurance packages (EAL) refer to CC Part 3 chapters 7.2 and 8
- On the assurance class ASE for Security Target evaluation refer to CC Part 3 chapter 12
- On the detailled definitions of the assurance components for the TOE evaluation refer to CC Part 3 chapters 13 to 17
- The table in CC part 3 , Annex E summarizes the relationship between the evaluation assurance levels (EAL) and the assurance classes, families and components.

The CC are published at http://www.commoncriteriaportal.org/cc/

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

Note: End of report