Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-1082-2020

for

Ciena 6500 Packet-Optical Platform Flex3 WaveLogic 3e OCLD Encryption Module, KM Firmware Version 2.01, ASIC Firmware Version 1.00

from

Ciena Corporation

sponsored by

Ciena Limited Germany

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-1082-2020 (*)

Network and Network related Devices and Systems

Ciena 6500 Packet-Optical Platform Flex3 WaveLogic 3e OCLD Encryption Module
KM Firmware Version 2.01, ASIC Firmware Version 1.00

from	Ciena Corporation
sponsored by	Ciena Limited Germany
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_FLR.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 5.

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, 27 October 2020

For the Federal Office for Information Security

Sandro Amendola
Head of Division

L.S.

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

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - 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

This page is intentionally left blank.

Contents

A. Certification

1. Preliminary Remarks

Under the BSIG[1] 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]

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 3 March 2005, Bundesgesetzblatt I, p. 519

- Common Criteria for IT Security Evaluation (CC), Version 3.1[4] [1] also published as ISO/IEC 15408.
- 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 Domain 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.sogis.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: https://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.

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

This certificate is recognized according to the rules of CCRA-2014, i. e. up to and including CC part 3 EAL 2+ ALC_FLR components. This certificate is recognized under CCRA-2014 for all assurance components selected.

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 Ciena 6500 Packet-Optical Platform Flex3 WaveLogic 3e OCLD Encryption Module, KM Firmware Version 2.01, ASIC Firmware Version 1.00 has undergone the certification procedure at BSI.

The evaluation of the product Ciena 6500 Packet-Optical Platform Flex3 WaveLogic 3e OCLD Encryption Module, KM Firmware Version 2.01, ASIC Firmware Version 1.00 was conducted by MTG AG. The evaluation was completed on 22 October 2020. MTG AG is an evaluation facility (ITSEF)[5] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Ciena Limited Germany.

The product was developed by: Ciena Corporation.

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 27 October 2020 is valid until 26 October 2025. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

[5] Information Technology Security Evaluation Facility

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,
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 Ciena 6500 Packet-Optical Platform Flex3 WaveLogic 3e OCLD Encryption Module, KM Firmware Version 2.01, ASIC Firmware Version 1.00 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] Ciena Corporation
7035 Ridge Road
Hannover, Maryland 21078
United States of America

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 the Ciena 6500 Flex3 WaveLogic 3e OCLD Encryption Module. The TOE is a cryptographic subsystem comprising firmware and hardware implemented as components on a line card or circuit pack (the Ciena 6500 Flex3 WaveLogic 3e OCLD Circuit Pack), which can be installed into the Ciena 6500 series Packet-Optical Platform. The TOE offers an integrated transport encryption solution providing protocol-agnostic 100 Gb/s or 200 Gb/s wire-speed encryption service.

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 augmented by ALC_FLR.2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.2. 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
Encryption	Plaintext user data is encrypted when entering the TOE and leaving the TOE as ciphertext data to ensure confidentiality during transfer to a peer device. The encryption key for this operation is kept confidential by the TOE.
Decryption	Ciphertext data sent from a peer device is decrypted when entering the TOE and leaving the TOE as plaintext data for the user. The decryption key for this operation is kept confidential by the TOE.
Digital signature creation	Digital signature creation supports authentication against the peer device. The signature-creation key is kept private by the TOE.
Digital signature verification	Digital signature verification allows authentication of the peer device. The signature verification key is authentically assigned to the holder of the signature-creation key and is public available to the verifier.
Cryptographic key management	The TOE manages the cryptographic keys necessary for its implemented cryptographic algorithms and protocols. The cryptographic key management controls the generation, storage, access and use of the cryptographic keys by the cryptographic functions. The cryptographic key management includes: ● Generation of random numbers using a deterministic random number generator seeded by a physical RNG ● Implementation of key generation algorithms depending on the intended use of the keys ● Secure storage of private keys protecting their confidentiality ● Key agreement protocols establishing ephemeral common secrets with external peer entities
Mutual authentication	The mutual authentication of communicating entities and the key agreement are combined to initiate and keep secure communication between trusted peer devices protecting the confidentiality of the transmitted user data.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapters 1.3.3 and 1.4.2.

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 3.2, 3.3 and 3.4.

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:

Ciena 6500 Packet-Optical Platform Flex3 WaveLogic 3e OCLD Encryption Module,
KM Firmware Version 2.01, ASIC Firmware Version 1.00

The following table outlines the TOE deliverables:

No	Type	Identifier	Article Number / Version	Form of Delivery
1	HW	● Krypto Module ● ASIC part number	● NTK53926-501, NTK53926-502 ● 077-0084-017, 077-0084-028	The TOE hardware parts are firm components on the Ciena 6500 Flex3 WaveLogic 3e OCLD (NTK539QS/NTK539QV variants) circuit packs. Shipment of the circuit pack to the customer is done with Ciena's standard carriers (e.g. FedEx).
2	FW	● KM Firmware ● ASIC Firmware	● 2.01 ● 1.00	TOE SW is readily installed on the TOE hardware, see #1
3	DOC	Security Target for the Ciena 6500 Flex3 WaveLogic 3e OCLD Encryption Module, 323-1851-CC-ST-NTK539QS-NTK539QV, Ciena Corporation [6] SHA2-256 Hash: 48eb44bb591e14c4cd5729fe6cdad7c0bce81f0ab153af4546dfb0d294609c94	Version 1.6	Download as PDF from portal my.ciena.com

No	Type	Identifier	Article Number / Version	Form of Delivery
4	DOC	Ciena 6500 Packet-Optical Platform, Release 12.3: WaveLogic Ai, Flex, 100G+, 40G, OSIC ISS, and SLIC10 Circuit Packs, Release 12.3, 323-1851-102.4 [8] SHA2-256 Hash: fb0c04be9b899cdf2f8817357faeb3e5c9cae04863e36859cb6ae8f58e2b41a5	Standard Issue 1, July 2018	Download as PDF from portal my.ciena.com
5	DOC	Ciena 6500 Packet-Optical Platform: “Installation - General Information”, Release 12.3, 323-1851-201.0 [9] SHA2-256 Hash: 8b46077a7384d5a01205b4e38032d2076e94051755ecc25449703e5569ac7a2d	Standard Issue 1, July 2018	Download as PDF from portal my.ciena.com
6	DOC	Ciena 6500 Packet-Optical Platform: “Administration and Security”, Release 12.3, 323-1851-301 [10] SHA2-256: 6e06e63de19335778f057a8ac8ec50c527c6a6d5e875463d2ca3b037ef1d1163	Standard Issue 2, September 2018	Download as PDF from portal my.ciena.com
7	DOC	Ciena 6500 Packet-Optical Platform: “TL-1 Command Definition”, Release 12.3, 323-1851-190 [11] SHA2-256: c98f421e8a24797e0ea69eab1dbd65ef885d5b540c2ab29aca7ca856ac8f297f	Standard Issue 1, July 2018	Download as PDF from portal my.ciena.com
8	DOC	Ciena 6500 Packet-Optical Platform: “MyCryptoTool Certificate Management and Quick Start”, Release 12.3, 323-1851-341 [12] SHA2-256: 00e27fb327d05d7ffcf05f3b378a57fb2aff61a456b485dad2aba5fab3423111	Standard Issue 1, July 2018	Download as PDF from portal my.ciena.com
9	DOC	Ciena 6500 Packet-Optical Platform: “Encryption and FIPS Security Policy Overview and Procedures”, Release 12.3, 323-1851-340 [13] SHA2-256: b88494f13b13ae9dccaeff12ac13bc66417b66f550b813e1ec1fd50014038fb0	Standard Issue 1, July 2018	Download as PDF from portal my.ciena.com

No	Type	Identifier	Article Number / Version	Form of Delivery
10	DOC	Ciena 6500 Flex3 WaveLogic 3e OCLD Encryption Module: FIPS 140-2 Non-Proprietary Security Policy [14] SHA2-256 Hash: b4ecfebc6017f1e1e3d391f3b898ce5dc03995828dd39ac818a8fe2b437aefc4	Version 1.1	Download as PDF from portal my.ciena.com

Table 2: Deliverables of the TOE

2.1. Overview of the delivery procedure

TOE Distribution and Shipment

The TOE hardware and firmware parts of the Ciena security product do not require any assembly or installation activities as they are delivered to the customer pre-installed on the (NTK539QS/NTK539QV variants, see #1 in table 2) circuit pack from the factory.

Shipment to the customer is done with Ciena's standard carriers (e.g. FedEx), i.e.:

- Ciena notifies the customer via email that the shipment will be sent by the carrier (FedEx, for example) with a dedicated shipment tracking number and an attached shipping document.
- The carrier notifies the customer via email of the expected delivery date and time containing the shipment tracking number.

Delivery of the TOE documentation is done through the customer downloading the TOE guidance documents from the my.ciena.com portal accessible for registered Ciena customers.

Acceptance of TOE by customer:

On receipt of the circuit pack containing the TOE, the customer's Crypto Officer / Administrator should:

- physically inspect the shipping for signs of damage
- check the package for any irregular tears or opening
- remove the shipping package
- compare the serial number of the circuit pack with the serial number on the separately mailed shipping document

If damage is found, the Crypto Officer / Administrator shall immediately contact Ciena using one of the following Ciena contact channels:

- support website
- support phone numbers
- support email address
- support specified in the customers sales contract
- sales account team assigned to the customer

The SHA2-256 hashes as listed in table 2 must be used to ensure data integrity during data transmission of the TOE documents downloaded.

If the hash values of the documents downloaded match the vales given in table 2 the documents are the correct ones. Otherwise the customer shall contact Ciena to get the authentic documents.

2.2. Identification of TOE by the customer

The TOE consists of hardware, firmware and documentation as listed in table 2.

The TOE hardware can be identified by checking the faceplate of the circuit pack that must be labelled with the text “NTK539QS” or “NTK539QV”.

The TOE’s firmware version can be retrieved by the administrator from the MyCryptoTool administration firmware. Each MyCryptoTool page shows in the bottom left corner the TOE version, i.e. “Version 2.01”. By default, the TOE version number is identical to the Krypto Module (KM) Firmware version.

The ASIC Firmware version (i.e. version 1.00) that is built into the Ciena OCLD Encryption Module TOE can be identified from the TOE version (i.e. 2.01) only by the developer, but not by the customer.

The TOE’s documentation files can be uniquely identified in the download area of the my.ciena.com portal using the name and references of the documents as listed in section 1.4.3.3 of the Security Target [6] or table 2 above.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues:

- Encryption of plaintext user data entering the TOE and leaving the TOE as ciphertext data to ensure confidentiality during transfer to a peer device. The encryption key for this operation is kept confidential by the TOE and is agreed with the peer device on a regular, manageable time interval.
- Decryption of ciphertext data sent from a peer device entering the TOE and leaving the TOE as plaintext data for the user. The decryption key for this operation is kept confidential by the TOE and is agreed with the peer device on a regular, manageable time interval.
- Digital signature creation to support authentication against the peer device. The signature creation key is kept private by the TOE.
- Digital signature verification, which allows authentication of the peer device. The signature verification key is authentically assigned to the holder of the signature-creation key and is available to the TOE as a trustworthy certificate. Digital signature verification of the TOE’s firmware assures the integrity and authenticity of the firmware during start-up.
- The TOE manages the cryptographic keys necessary for its implemented cryptographic algorithms and protocols. The cryptographic key management controls the generation, storage, access and use of the cryptographic keys by the cryptographic functions.
- The TOE provides mutual peer authentication between the TOE and the peer device connected via Optical Transport Network (OTN).

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. The following topics are of relevance:

- Those responsible for the operation of the TOE must ensure that management and configuration of the security functions of the TOE is undertaken by non-evil, trusted administrators trained in the secure operation of the TOE.
- Management tools used by the administrator (e.g. Web Browser) must be non-evil and trustworthy.
- The ECC device certificate necessary for identifying the TOE during IKEv2 message exchange must be signed by a trustworthy CA with a strong ECC key pair from the NIST P-384 (secp384r1) elliptic curve.
- The developer key pair used for signing the TOE firmware must be a cryptographically strong ECC key pair from the NIST P-384 (secp384r1) elliptic curve signed by a trustworthy CA.
- All non-TOE parts of the Flex3 WL3e OCLD circuit pack are trustworthy and do not compromise the security functionality of the TOE.
- Keys generated at the factory must be strong random numbers and are brought into the TOE in a secure production environment by the manufacturer.
- The real time clock in the TOE environment provides reliable time services for the TOE. This shall be achieved by regular time synchronization with NTP time server(s).
- The TOE must be installed in a non-public environment which is physically secure. Only authorized individuals may physically access the TOE.

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The following 1 shows the architectural decomposition of the TOE in terms of subsystems.

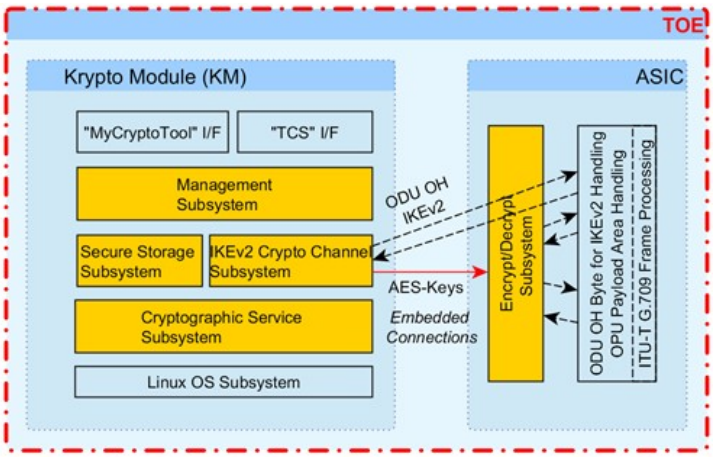

Figure 1: TOE subsystems

Physically the WL3E OCLD TOE consists of the Krypto Module (KM) and an ASIC. Both hardware components are connected on the circuit pack with an embedded wire connection.

Logically the TOE consists of several subsystems. The SFR-enforcing subsystems are the:

Cryptographic Service Subsystem
This subsystem implements cryptographic functions (RNG, ECC key agreement, ECC key generation, ECDSA signature generation and verification) used by other subsystems.

IKEv2 Crypto Channel Subsystem
Here the IKE (Internet Key Exchange) v2 protocol is implemented to provide peer-to-peer authentication with X.509 certificates and to calculate periodically common shared secrets to derive the symmetric encryption/decryption keys for the user data.

Secure Storage Subsystem
The Secure Storage Subsystem provides certificates storage and provisioning data storage in non-volatile memory. It protects the confidentiality of security parameters (e.g. the private key of the authentication certificate).

Encrypt/Decrypt Subsystem
The “Encrypt/Decrypt Subsystem” provides user data encryption/decryption with the keys set by the “IKEv2 Crypto Channel Subsystem”.

Management Subsystem
The “Management Subsystem” provides a library of APIs that allow the “MyCryptoTool I/F” and the “TCS I/F” to interact with the rest of KM software components through messaging for handling administrator’s requests. Management of X.500 certificates, IKEv2-parameters setting and firmware loading is implemented in this subsystem.

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

7.1. Test Configuration

The ”Flex3 WL3e OCLD” circuit pack TOE consists of the following components:

TOE Hardware	• Krypto Module (part number NTK53926-501, NTK53926-502) and • ASIC (part number 077-0084-017, 077-0084-028) on the Ciena 6500 Flex3 WaveLogic 3e OCLD (NTK539QS/NTK539QV variants) circuit packs
TOE Firmware	• KM Firmware Version 2.01

Table 3: TOE components

The tested TOE is part of the “Flex3 WL3e OCLD” circuit pack which are plugged into and operated in a shelf of the Ciena 6500 Packet-Optical Platform at the Ciena test lab in Ottawa. A second shelf was configured to operate as a peer to the shelf containing the

TOE, creating a loopback for data received from the TOE and provide the possibility to test parameters related to the TOE's communication channel setup.

Only the NTK539QS circuit pack variant has been used in the test configuration.

The following figure shows how the TOE provided by the developer has been embedded into the overall testing environment:

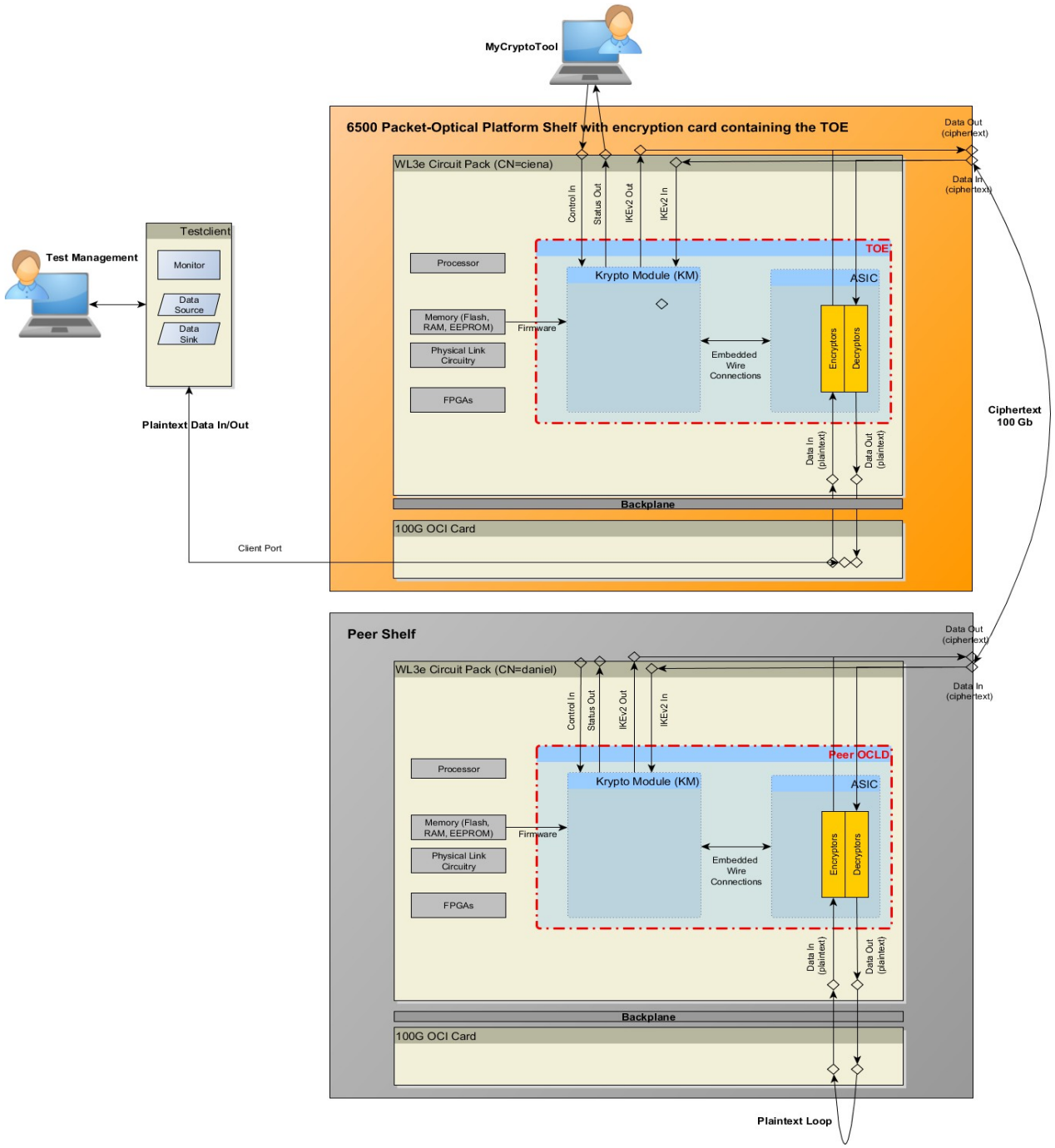

Figure 2: TOE test setup

The test setup consists of two 6500 Packet-Optical Platform shelves. Each shelf is equipped with a 100G OCI card for client access and a Flex3 WL3e OCLD circuit pack

containing the TOE. The encrypted line ports of both encryption cards are connected via an optical fibre link.

The TOE (i.e. the circuit pack with the TOE) is connected via the shelf-backplane and the OCI card to a test client sending and receiving sample user data. The plaintext user data is encrypted by the TOE and sent to the peer. The peer decrypts the data, sends it via the shelf-backplane to the OCI client interface where the received data is echoed back (plaintext loop). On the way back to the test client the echoed data is encrypted again by the peer device and decrypted within the TOE.

Connection monitoring, certificate management and crypto parameter configuration on the TOE has been done with the MyCryptoTool as shown in the figure above.

The TOE was installed and configured according to the guidance and configuration as described in the ST [6] when the testing was performed.

7.2. Developer tests according to ATE_FUN

The developer performed cryptographic tests to verify the claimed security functionality from the Security Target [6].

The developer provided test documentation consists of the test vectors and their result files for all cryptographic algorithms implemented by the TOE. The developer tests have also been used for the TOE's FIPS 140-2 certification, i.e. test sessions for AES, AES_GCM, SHA, ECDSA2, CTR_DRBG, HMAC, KDF have been conducted by the developer.

The evaluator checked and verified on site at Ciena that the TOE as specified in the ST [6] has really been installed and has been used within the Ciena test environment for their tests.

7.3. Independent testing according to ATE_IND

For independent testing the evaluator specified test cases with the intention to cover all SFRs from the ST. For that purpose, all of the developer's KAT tests (Known Answer Test) on cryptographic algorithms have been repeated with unknown cryptographic test vectors and comprehensive own test cases have been specified, especially covering the management and administration functions of the TOE.

For test case specification and test case execution documentation the evaluator used the Open Source based test management tool "TestLink".

The independent testing was performed in the test environment that has been installed and configured at the developer's test lab in Ottawa. Some developer provided tests were carried out by Ciena personnel in the Ciena test laboratory in Ottawa under the supervision of the evaluators.

During independent testing the evaluators specified, run and evaluated test cases covering all SFRs from the ST. The results of those tests showed that all claimed SFRs are achieved by the TOE.

Using this test environment when executing the evaluator's tests, the overall test result was that no deviations were found between the expected and the actual test results.

7.4. Penetration Testing according to AVA_VAN

The approach chosen by the evaluators is appropriate for the assurance component AVA_VAN.2, requiring the resistance of the TOE to an attack with the Basic attack potential. First the evaluators used publicly available sources to identify potential vulnerabilities in the TOE.

In addition, the evaluators applied an “unstructured analysis” while evaluating the developer provided Common Criteria evidence documentation to identify potential vulnerabilities applicable to the TOE.

The evaluators analysed which of the potential vulnerabilities identified in the steps above are not applicable to the TOE in its operational environment. For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluators devised the attack scenarios where these potential vulnerabilities could be exploited.

For each such attack scenario they first performed a theoretical analysis on the related attack potential, concluding that there are no attack scenarios where the required attack potential is *Basic*.

None of the attack scenarios developed and analysed has been considered for further testing, as the assumed attack potential for each scenario is beyond a Basic attacker. Thus, no penetration testing was actually performed.

For penetration testing the evaluators therefore put emphasis on attack scenarios that would allow an attacker to bypass the overall security functionality of the TOE.

Being resistant against attack vectors with Basic attack potential shows that the TOE, when installed and configured as described in the operational guidance documentation, can be operated in a secure and trustworthy manner.

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

8. Evaluated Configuration

This certification covers the following configurations of the TOE: The TOE is part of the “Flex3 WL3e OCLD” circuit pack. The difference between the QS and QV circuit pack variants is essentially the optical performance on the DWDM line side - the QS is rated for long haul reach (1000s of km) vs. metro reach (~300 km) for the QV variant. There is no difference in the TOE’s firmware between both circuit pack variants. For more information, see the test configuration in chapter 7.1.

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 components ALC_FLR.2 augmented for this TOE evaluation.

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 augmented by ALC_FLR.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	Key Size in Bits	Security Level above 100 Bits
1	Key Derivation (IKEv2)	PRF-HMAC-SHA-384	FIPS 180-4, Secure Hash Standard (SHS), 2015 (SHA), RFC 2104 (HMAC), RFC-4868, RFC-7296, Sec. 2.13, 2.14, 2.17	|k| = 384	yes
2	Key Agreement (IKEv2)	Elliptic Curve Key Agreement - Diffie Hellman	ANSI X9.63 (Key Agreement and Key Transport Using Elliptic Curve Cryptography) RFC-5903, Sec. 3.2	Key size for elliptic curve - secp384r1, i.e. |k| = 384	yes
3	Authentication (IKEv2)	ECDSA-signature generation and verification	FIPS PUB 186-4, Digital Signature Stand-ard (DSS), Section 6 and Appendix D,	Key size for elliptic curve - secp384r1, i.e. |k| = 384	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
		using SHA-384	Implementing “NIST curves” P-384; ISO/IEC 14888-3, Section 6.4, for ECDSA schemes RFC-4754 RFC-7296, Sec. 2.15		
4	Confidentiality/ Integrity (IKEv2)	AES in GCM mode	FIPS 197 (AES) NIST-SP800-38D (GCM) RFC-5282	|k| = 256	yes
5	Confidentiality (data path)	AES in CTR mode	FIPS 197 (AES) NIST-SP800-38A (CTR)	|k| = 256	yes
6	Confidentiality (key)	AES in CBC mode	FIPS 197 (AES) NIST-SP800-38A (CBC)	|k| = 256	yes
7	Authenticity (Firmware)	ECDSA-signature verification using SHA-384	FIPS PUB 186-4, Digital Signature Standard (DSS), Section 6 and Appendix D, Implementing “NIST curves” P-384; ISO/IEC 14888-3, Section 6.4, for ECDSA schemes	Key size for elliptic curve - secp384r1, i.e. |k| = 384	yes
8	Authenticity (Certificates)	ECDSA-signature verification using SHA-384	FIPS PUB 186-4, Digital Signature Stand-ard (DSS), Section 6 and Appendix D, Implementing “NIST curves” P-384; ISO/IEC 14888-3, Section 6.4, for ECDSA schemes	Key size for elliptic curve - secp384r1, i.e. |k| = 384	yes
9	Random Number Generation (DRG.2)	CTR_DRBG (AES)	NIST SP 800-90A using CTR_DRBG (AES) seeded by an entropy source that accumulates entropy from one independent TSF-hardware-based noise source	None	n.a.

Table 4: TOE cryptographic functionality

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.

12. Regulation specific aspects (eIDAS, QES)

None

13. Definitions

13.1. Acronyms

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
ASIC	Application-Specific Integrated Circuit
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
CCRA	Common Criteria Recognition Arrangement
CBC	Cipher Block Chaining
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
CTR	Counter
DRBG	Deterministic Random Bit Generator
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCM	Galois/Counter Mode
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility

KAT	Known Anser Test
KEK	Key Encrypting Key
KM	Krypto Module
NIST	National Institute of Standards and Technology
OCLD	Optical Channel Laser and Detector
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TCS	Transport Control Subsystem
TOE	Target of Evaluation
TSF	TOE Security Functionality
WL3e	WaveLogic 3 Extreme

13.2. 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.

14. 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
https://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 5, April 2017, https://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-1082-2020, Security Target for the Ciena 6500 Packet-Optical Platform Flex3 WaveLogic 3e OCLD Encryption Module, Doc-ID: 323-1851-CC-ST-NTK539QS-NTK539QV, Version 1.6, Ciena Corporation, April 28, 2020

[7] Evaluation Technical Report, ETR Part Summary, Ciena OCLD Encryption Module, Version 1.1, October 10, 2020, MTG (confidential document)

[8] Ciena 6500 Packet-Optical Platform, Release 12.3: WaveLogic Ai, Flex, 100G+, 40G, OSIC ISS, and SLIC10 Circuit Packs, Release 12.3, 323-1851-102.4, Standard Issue 1, July 2018

[9] Ciena 6500 Packet-Optical Platform: “Installation - General Information”, Release 12.3, 323-1851-201.0, Standard Issue 1, July 2018

[10] Ciena 6500 Packet-Optical Platform: “Administration and Security”, Release 12.3, 323-1851-301, Standard Issue 2, September 2018

[11] Ciena 6500 Packet-Optical Platform: “TL-1 Command Definition”, Release 12.3, 323-1851-190, Standard Issue 1, July 2018

[12] Ciena 6500 Packet-Optical Platform: “MyCryptoTool Certificate Management and Quick Start”, Release 12.3, 323-1851-341, Standard Issue 1, July 2018

[13] Ciena 6500 Packet-Optical Platform: “Encryption and FIPS Security Policy Overview and Procedures”, Release 12.3, 323-1851-340, Standard Issue 1, July 2018

[14] Ciena 6500 Flex3 WaveLogic 3e OCLD Encryption Module: FIPS 140-2 Non-Proprietary Security Policy, Version 1.1

[7] specifically

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

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 https://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