Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti ICT
(DPCM del 30 ottobre 2003 - G.U. n. 93 del 27 aprile 2004)

Certificato n. 1/19

(Certification No.)

Prodotto: *(Product)* **CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware**

Sviluppato da: *(Developed by)* **Certes Networks, Inc.**

Il prodotto indicato in questo certificato è risultato conforme ai requisiti dello standard ISO/IEC 15408 (Common Criteria) v. 3.1 per il livello di garanzia:

The product identified in this certificate complies with the requirements of the standard ISO/IEC 15408 (Common Criteria) v. 3.1 for the assurance level:

EAL4+
(ALC_FLR.3)

Il Direttore
(Dott.ssa Rita Forsi)

Roma, 13 marzo 2019

Fino a EAL2 *(Up to EAL2)*

Common Criteria

SOGIS IT SECURITY CERTIFIED

Fino a EAL4 *(Up to EAL4)*

This page is intentionally left blank

Ministero dello Sviluppo Economico

Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione

Organismo di Certificazione della Sicurezza Informatica

Certification Report

CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware

OCSI/CERT/CCL/07/2018/RC

Version 1.0

13 March 2019

Courtesy translation

Disclaimer: this translation in English language is provided for informational purposes only; it is not a substitute for the official document and has no legal value. The original Italian language version of the document is the only approved and official version.

1 Document revisions

Version	Author	Information	Date
1.0	OCSI	First issue	13/03/2019

2 Table of contents

3 Acronyms

CC Common Criteria

CCRA Common Criteria Recognition Arrangement

CEM Common Evaluation Methodology

CEP Certes Enforcement Point

CLI Command Line Interface

DPCM Decreto del Presidente del Consiglio dei Ministri

EAL Evaluation Assurance Level

FIPS Federal Information Processing Standard

GUI Graphical User Interface

HW Hardware

LAN Local-Area Network

LGP Linea Guida Provvisoria

LVS Laboratorio per la Valutazione della Sicurezza

NIS Nota Informativa dello Schema

NTP Network Time Protocol

OCSI Organismo di Certificazione della Sicurezza Informatica

PP Protection Profile

RFV Rapporto Finale di Valutazione (Evaluation Technical Report)

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

SSH Secure Shell

SW Software

TDS Traguardo di Sicurezza (Security Target)

TLS Transport Layer Security

TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
WAN	Wide-Area Network

4 References

4.1 Criteria and regulations

[CC1] CCMB-2017-04-001, “Common Criteria for Information Technology Security Evaluation, Part 1 – Introduction and general model”, Version 3.1, Revision 5, April 2017

[CC2] CCMB-2017-04-002, “Common Criteria for Information Technology Security Evaluation, Part 2 – Security functional components”, Version 3.1, Revision 5, April 2017

[CC3] CCMB-2017-04-003, “Common Criteria for Information Technology Security Evaluation, Part 3 – Security assurance components”, Version 3.1, Revision 5, April 2017

[CCRA] “Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security”, July 2014

[CEM] CCMB-2017-04-004, “Common Methodology for Information Technology Security Evaluation – Evaluation methodology”, Version 3.1, Revision 5, April 2017

[LGP1] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Descrizione Generale dello Schema Nazionale - Linee Guida Provvisorie - parte 1 – LGP1 versione 1.0, Dicembre 2004

[LGP2] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Accreditamento degli LVS e abilitazione degli Assistenti - Linee Guida Provvisorie - parte 2 – LGP2 versione 1.0, Dicembre 2004

[LGP3] Schema nazionale per la valutazione e certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell’informazione - Procedure di valutazione - Linee Guida Provvisorie - parte 3 – LGP3, versione 1.0, Dicembre 2004

[NIS1] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 1/13 – Modifiche alla LGP1, versione 1.0, Novembre 2013

[NIS2] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 2/13 – Modifiche alla LGP2, versione 1.0, Novembre 2013

[NIS3] Organismo di Certificazione della Sicurezza Informatica, Nota Informativa dello Schema N. 3/13 – Modifiche alla LGP3, versione 1.0, Novembre 2013

[SOGIS] “Mutual Recognition Agreement of Information Technology Security Evaluation Certificates”, Version 3, January 2010

4.2 Technical documents

[CEP] "CEP User Guide v5.3", Revision A, April 2018

[CFNC] "CFNC User Guide v5.3", Revision A, 20 April 2018

[DEL] "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Secure Delivery Document, v0.2, 15 November 2018

[INST] "CryptoFlow Net Creator v5.3" Installation Guide, Revision A, April 2018

[RFV] "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Evaluation Technical Report, v1, 29 January 2019

[SUP] "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Guidance Documentation Supplement, v0.5, 22 January 2019

[TDS] "CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Security Target, v0.7, 22 January 2019

5 Recognition of the certificate

5.1 European Recognition of CC Certificates (SOGIS-MRA)

The European SOGIS-Mutual Recognition Agreement (SOGIS-MRA, version 3 [SOGIS]) became effective in April 2010 and provides mutual recognition of certificates based on the Common Criteria (CC) Evaluation Assurance Level up to and including EAL4 for all IT-Products. A higher recognition level for evaluations beyond EAL4 is provided for IT-Products related to specific Technical Domains only.

The current list of signatory nations and of technical domains for which the higher recognition applies and other details can be found on http://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognized under the terms of this agreement by signatory nations.

This certificate is recognized under SOGIS-MRA up to EAL4.

5.2 International Recognition of CC Certificates (CCRA)

The current version of the international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, [CCRA] has been ratified on 08 September 2014. It covers CC certificates compliant with collaborative Protection Profiles (cPP), up to and including EAL4, or certificates based on assurance components up to and including EAL 2, with the possible augmentation of Flaw Remediation family (ALC_FLR).

The current list of signatory nations and of collaborative Protection Profiles (cPP) and other details can be found on http://www.commoncriteriaportal.org.

The CCRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by signatory nations.

This certificate is recognised under CCRA up to EAL2.

6 Statement of Certification

The Target of Evaluation (TOE) is the product “CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware”, short name “CryptoFlow Net Creator v5.3”, developed by Certes Networks, Inc.

The TOE is a suite of components consisting of CEP encryption appliances, configured and managed using the CryptoFlow Net Creator custom-written application software. All of the security features of the TOE, including the cryptographic algorithms, are implemented in the CryptoFlow Net Creator v5.3 Software and the CEP v5.3 Firmware. No security features of the TOE are implemented in the TOE hardware.

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guidelines [LGP1, LGP2, LGP3] and Scheme Information Notes [NIS1, NIS2, NIS3]. The Scheme is operated by the Italian Certification Body “Organismo di Certificazione della Sicurezza Informatica (OCSI)”, established by the Prime Minister Decree (DPCM) of 30 October 2003 (O.J. n.98 of 27 April 2004).

The objective of the evaluation is to provide assurance that the product complies with the security requirements specified in the associated Security Target [TDS]; the potential consumers of the product should review also the Security Target, in addition to the present Certification Report, in order to gain a complete understanding of the security problem addressed. The evaluation activities have been carried out in accordance with the Common Criteria Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The TOE resulted compliant with the requirements of Part 3 of the CC v 3.1 for the assurance level EAL4, augmented with ALC_FLR.3, according to the information provided in the Security Target [TDS] and in the configuration shown in Annex B – Evaluated configuration of this Certification Report.

The publication of the Certification Report is the confirmation that the evaluation process has been conducted in accordance with the requirements of the evaluation criteria Common Criteria - ISO/IEC 15408 ([CC1], [CC2], [CC3]) and the procedures indicated by the Common Criteria Recognition Arrangement [CCRA] and that no exploitable vulnerability was found. However the Certification Body with such a document does not express any kind of support or promotion of the TOE.

7 Summary of the evaluation

7.1 Introduction

This Certification Report states the outcome of the Common Criteria evaluation of the product "CryptoFlow Net Creator v5.3" to provide assurance to the potential consumers that TOE security features comply with its security requirements.

In addition to the present Certification Report, the potential consumers of the product should review also the Security Target [TDS], specifying the functional and assurance requirements and the intended operational environment.

7.2 Executive summary

TOE name	CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware
Security Target	"CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware" Security Target, v0.7, 22 January 2019
Evaluation Assurance Level	EAL4 augmented with ALC_FLR.3
Developer	Certes Networks, Inc.
Sponsor	Corsec Security, Inc.
LVS	CCLab Software Laboratory
CC version	3.1 Rev. 5
PP conformance claim	No compliance declared
Evaluation starting date	25 September 2018
Evaluation ending date	29 January 2019

The certification results apply only to the version of the product shown in this Certification Report and only if the operational environment assumptions described in the Security Target [TDS] are fulfilled.

7.3 Evaluated product

This section summarizes the main functional and security requirements of TOE; for a detailed description, please refer to the Security Target [TDS].

The TOE is a suite of components consisting of CEP encryption appliances and CryptoFlow Net Creator central security and policy management software. CryptoFlow Net Creator is a web-based GUI that configures and monitors the CEP encryption appliances, stores and deploys policies (or rules), and provides key management and auditing capabilities. Policies created and distributed by CryptoFlow Net Creator define the actions CEPs take on protected network traffic, either to encrypt and decrypt it, send it in the clear, or drop it. All remote management traffic transmitted between the CryptoFlow Net Creator and CEP encryption appliances is protected via TLSv1.2 sessions.

The CEP encryption appliance provides high-speed processing capabilities to protect data travelling over untrusted networks while in transit between sites. Each CEP encryption appliance has one management port and two data ports. A local data port is used for LAN connections to trusted networks, while a remote data port provides WAN connections over untrusted networks. Unencrypted traffic that originates from a trusted, local network is received on the local data port of the origination CEP.

The CryptoFlow Net Creator GUI is the primary management interface. It is a web-based application and database server supporting role-based access that is used to provision CEP encryption appliances, define polices, and manage keys and certificates. Policies and key data, used by the CEPs to derive encryption keys, are generated and securely distributed to CEP encryption appliances via a TLS authenticated and encrypted channel, with the option for bilateral certificate-based authentication.

Figure 1 shows the details of the deployment configuration of the TOE.

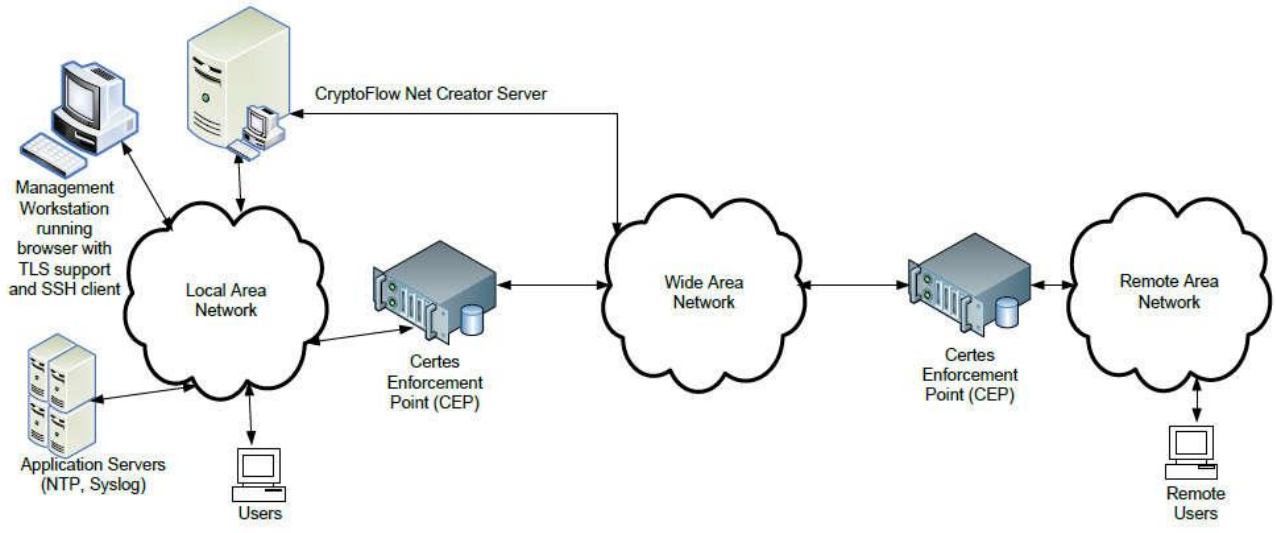

Figure 1 – Deployment Configuration of the TOE

For a detailed description of the TOE, consult sect. 1.4 and 1.5 of the Security Target [TDS]. The most significant aspects are summarized below.

7.3.1 TOE Architecture

The CEPs can be managed by authorized administrators using the CryptoFlow Net Creator GUI or the CEP CLI. Using the CryptoFlow Net Creator GUI, an administrator can configure and manage multiple appliances from a single centralized location. In addition, security policies defining how and where the encryption will take place can be created. The CEP CLI can be accessed from the management workstation either directly via a serial port or through an SSH connection. It allows an administrator to perform initial setup and troubleshooting of the CEP.

A policy defines networks to be protected and groups these networks to form Network Sets. A policy can have one or more Network Sets associated with it. Once the Network Sets are established, CEPs can be assigned to those Network Sets and the security policies governing them are defined. Each CEP in a given network is given the same group encryption key data to be used to derive encryption keys. CryptoFlow Net Creator centralizes the creation and distribution of key data and policies. In addition, it provides a rekeying capability that ensures that CEPs generate new encryption keys at defined rekey intervals.

The TOE is intended to be deployed in a physically secure cabinet or data center with the appropriate level of physical access control and physical protection (e.g., fire control, locks, alarms). The TOE is intended to be managed by administrators operating under a consistent security policy.

The TOE is meant to provide confidentiality and integrity services to information traveling across an untrusted network. The TOE environment should ensure stable network connectivity for the TOE to perform its intended function.

The TOE requires reliable timestamps to audit its security-relevant events. The TOE requires the clocks on the different components of the TOE to be synchronized so that the time each event occurred can be accurately audited. The TOE environment is responsible for providing an NTP server for time synchronization.

The TOE management functionality is accessed via an independent third-party SSH client or Web browser.

Figure 2 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the TOE. The TOE is a software and hardware TOE. The TOE is a CEP encryption appliance (both hardware and software) configured and managed using the CryptoFlow Net Creator custom-written application software.

Only the CEP (hardware and software) and CryptoFlow Net Creator (software-only) are included in the TOE boundary. The CEP hardware includes purpose-built appliances that are included with the purchase of the TOE. The software is custom-made to provide cryptographic functionality and the ability to manage the CEP encryption appliances.

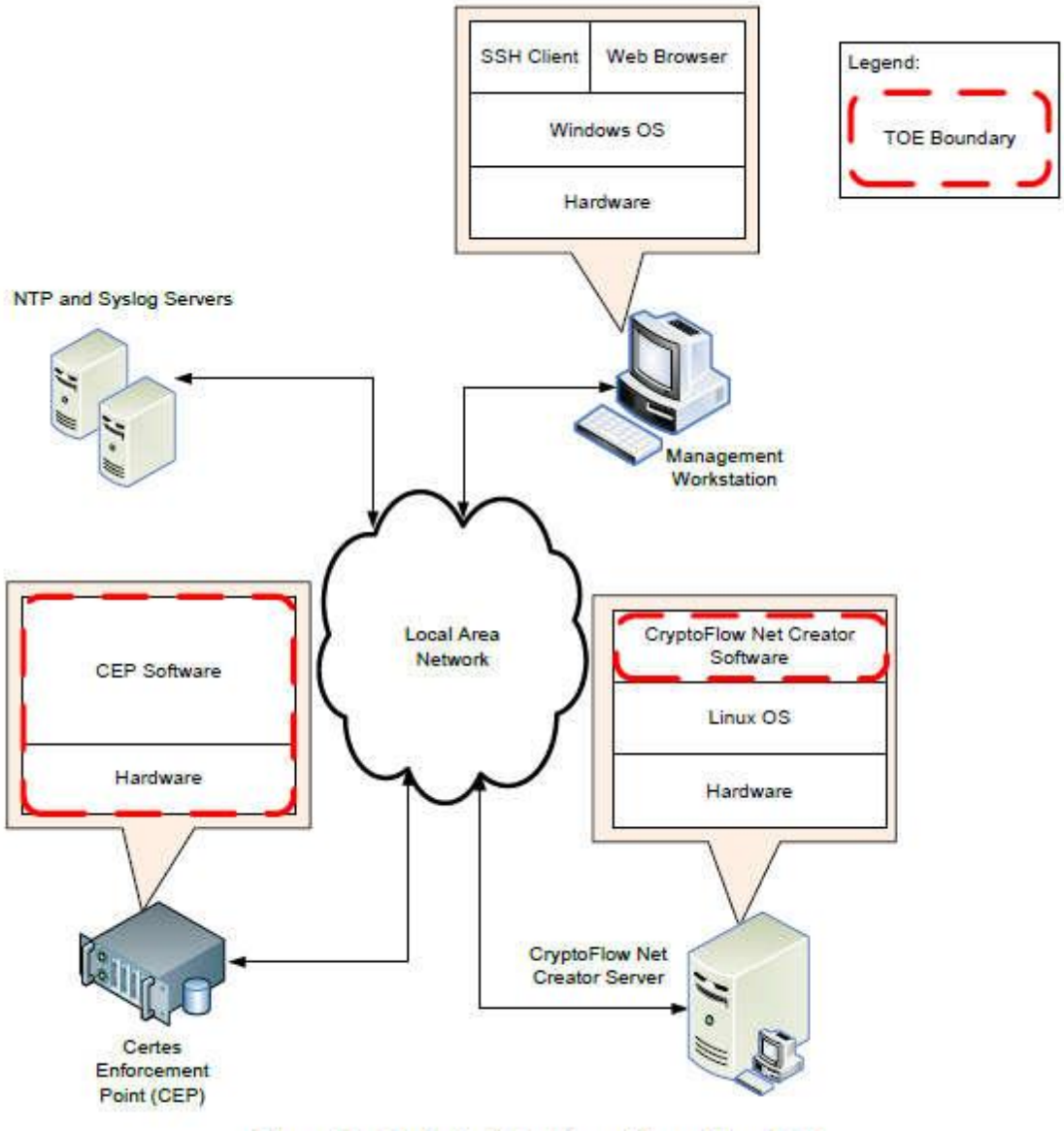

Figure 2 – Physical TOE boundary

7.3.2 TOE security features

The Security Problem of the TOE, including security objectives, assumptions, threats and organizational security policies, is defined in sect. 3 of the Security Target [TDS].

All of the security features of the TOE, including the cryptographic algorithms, are implemented in the CryptoFlow Net Creator v5.3 Software and the CEP v5.3 Firmware. No security features of the TOE are implemented in the TOE hardware. In addition, the security features are the same amongst all the TOE CEP encryption appliance models.

For a detailed description of the TOE Security Functions, consult sect. 7.1 of the Security Target [TDS]. The most significant aspects are summarized below.

- **Security Audit.** The TOE provides functionality for the generation and viewing of audit records. As administrators manage and configure the TOE, the TOE tracks

their activities by recording audit records in audit logs. The TOE records all security-relevant configuration settings and changes to ensure accountability of the administrator's actions. Authorized administrators can view the audit records, showing the identity of the user that triggered the event.

- **Cryptographic Support.** The TOE uses two FIPS 140-2 validated cryptographic modules to perform cryptographic operations. The cryptographic operations are used to secure communications from remote administrators at the CryptoFlow Net Creator GUI and CEP CLI. They are also used to encrypt user data, create a secure communication channel for the transfer of user data between CEPs, and protect TSF data (e.g., key data, policies) transmitted between CryptoFlow Net Creator and the CEPs.

- **User Data Protection.** The TOE enforces the Information Flow Control SFP that applies a set of rules to traffic passing through the TOE. Depending on the operation identified in the SFP, the TOE will determine whether to pass user traffic in the clear, discard it, or encrypt/decrypt it. Authorized TOE administrators configure the SFP by setting security attributes using the CryptoFlow Net Creator GUI or the CEP CLI.

- **Identification and Authentication.** All TOE administrators must be identified and authenticated prior to performing any actions at the CryptoFlow Net Creator GUI or CEP CLI. Access to the TOE requires an authorized username and role. This ensures that only legitimate administrators of the TOE can gain access to the configuration and management settings. The TOE obscures passwords at the CryptoFlow Net Creator GUI and CEP CLI during authentication.

- **Security Management.** The TOE is managed by administrators in one of eight roles: Platform Administrator, Administrator, Appliance Administrator, Appliance Operator, Policy Creator, Policy Deployer, User, and Ops. The TOE is capable of performing the following management functions: managing the Information Flow Control SFP security attributes and managing TSF data. The TOE restricts access to management functions based on the administrator's role. The Information Flow Control SFP is permissive by default, allowing information to pass between CEPs in the clear; however, authorized administrators are able to modify the Information Flow Control SFP to perform alternative operations, like dropping or encrypting the information.

- **Protection of TOE Security Functionality.** The TOE protects TSF data from disclosure and modification when it is transmitted between separate parts of the TOE. The TOE uses TLSv1.2 to secure communication between CryptoFlow Net Creator and a CEP encryption appliance. The TOE and TOE environment provide reliable timestamps for the CEP encryption appliance and CryptoFlow Net Creator software, respectively. The timestamps are used to record accurate time for audit records. The time for all TOE components is synchronized using an NTP server in the TOE environment.

- **TOE Access.** The TOE terminates an inactive administrator CryptoFlow Net Creator GUI or CEP CLI session after a preconfigured time period. Administrators must re-authenticate after being logged out. This prevents an unauthorized individual from gaining access to the TOE management functions through an

unattended session. Administrators may also terminate their own interactive sessions. Before establishing a user session, the TOE displays a login banner containing an advisory warning message regarding unauthorized use of the TOE.

- **Trusted Path/Channels.** The TOE (CEP encryption appliance) provides a trusted channel between itself and another trusted product (another CEP encryption appliance in this case) by encrypting and decrypting and authenticating all transmitted data using cryptographic algorithms provided by a FIPS 140-2 validated cryptographic module. It uses this trusted channel to transfer user between CEP encryption appliances. Using a supported web browser, a remote administrator initiates a secure connection to the CryptoFlow Net Creator GUI.

7.4 Documentation

The guidance documentation specified in Annex A – Guidelines for the secure usage of the product is delivered to the customer together with the product.

The guidance documentation contains all the information for secure initialization, configuration and secure usage the TOE in accordance with the requirements of the Security Target [TDS].

Customers should also follow the recommendations for the secure usage of the TOE contained in sect. 8.2 of this report.

7.5 Protection Profile conformance claims

The Security Target [TDS] does not claim conformance to any Protection Profile.

7.6 Functional and assurance requirements

All Security Functional Requirements (SFR) have been selected from CC Part 2 [CC2].

All Security Assurance Requirements (SAR) have been selected from CC Part 3 [CC3].

Please refer to the Security Target [TDS] for the complete description of all security objectives, the threats that these objectives should address, the Security Functional Requirements (SFR) and the security functions that realize the same objectives.

7.7 Evaluation conduct

The evaluation has been conducted in accordance with the requirements established by the Italian Scheme for the evaluation and certification of security systems and products in the field of information technology and expressed in the Provisional Guideline [LGP3] and the Scheme Information Note [NIS3] and in accordance with the requirements of the Common Criteria Recognition Arrangement [CCRA].

The purpose of the evaluation is to provide assurance on the effectiveness of the TOE to meet the requirements stated in the relevant Security Target [TDS]. Initially the Security Target has been evaluated to ensure that constitutes a solid basis for an evaluation in accordance with the requirements expressed by the standard CC. Then, the TOE has been evaluated on the basis of the statements contained in such a Security Target. Both

phases of the evaluation have been conducted in accordance with the CC Part 3 [CC3] and the Common Evaluation Methodology [CEM].

The Certification Body OCSI has supervised the conduct of the evaluation performed by the evaluation facility (LVS) CCLab Software Laboratory.

The evaluation was completed on 29 January 2019 with the issuance by LVS of the Evaluation Technical Report [RFV], which was approved by the Certification Body on 26 February 2019. Then, the Certification Body issued this Certification Report.

7.8 General considerations about the certification validity

The evaluation focused on the security features declared in the Security Target [TDS], with reference to the operating environment specified therein. The evaluation has been performed on the TOE configured as described in Annex B – Evaluated configuration. Potential customers are advised to check that this corresponds to their own requirements and to pay attention to the recommendations contained in this Certification Report.

The certification is not a guarantee that no vulnerabilities exist; it remains a probability (the smaller, the higher the assurance level) that exploitable vulnerabilities can be discovered after the issuance of the certificate. This Certification Report reflects the conclusions of the certification at the time of issuance. Potential customers are invited to check regularly the arising of any new vulnerability after the issuance of this Certification Report, and if the vulnerability can be exploited in the operational environment of the TOE, check with the developer if security updates have been developed and if those updates have been evaluated and certified.

8 Evaluation outcome

8.1 Evaluation results

Following the analysis of the Evaluation Technical Report [RFV] issued by the LVS CCLab Software Laboratory and documents required for the certification, and considering the evaluation activities carried out, the Certification Body OCSI concluded that TOE "CryptoFlow Net Creator v5.3" meets the requirements of Part 3 of the Common Criteria [CC3] provided for the evaluation assurance level EAL4, augmented with ALC_FLR.3, with respect to the security features described in the Security Target [TDS] and the evaluated configuration, shown in Annex B – Evaluated configuration.

Table 1 summarizes the final verdict of each activity carried out by the LVS in accordance with the assurance requirements established in [CC3] for the evaluation assurance level EAL4, augmented with ALC_FLR.3.

Assurance classes and components		**Verdict**
Security Target evaluation	**Class ASE**	Pass
Conformance claims	ASE_CCL.1	Pass
Extended components definition	ASE_ECD.1	Pass
ST introduction	ASE_INT.1	Pass
Security objectives	ASE_OBJ.2	Pass
Derived security requirements	ASE_REQ.2	Pass
Security problem definition	ASE_SPD.1	Pass
TOE summary specification	ASE_TSS.1	Pass
Development	**Class ADV**	Pass
Security architecture description	ADV_ARC.1	Pass
Complete functional specification	ADV_FSP.4	Pass
Implementation representation of the TSF	ADV_IMP.1	Pass
Basic modular design	ADV_TDS.3	Pass
Guidance documents	**Class AGD**	Pass
Operational user guidance	AGD_OPE.1	Pass
Preparative procedures	AGD_PRE.1	Pass
Life cycle support	**Class ALC**	Pass
Production support, acceptance procedures and automation	ALC_CMC.4	Pass
Problem tracking CM coverage	ALC_CMS.4	Pass

Assurance classes and components		Verdict
Delivery procedures	ALC_DEL.1	Pass
Identification of security measures	ALC_DVS.1	Pass
Systematic flaw remediation	ALC_FLR.3	Pass
Developer defined life-cycle model	ALC_LCD.1	Pass
Well-defined development tools	ALC_TAT.1	Pass
Test	**Class ATE**	Pass
Analysis of coverage	ATE_COV.2	Pass
Testing: basic design	ATE_DPT.1	Pass
Functional testing	ATE_FUN.1	Pass
Independent testing - sample	ATE_IND.2	Pass
Vulnerability assessment	**Class AVA**	Pass
Focused vulnerability analysis	AVA_VAN.3	Pass

Table 1 – Final verdicts for assurance requirements

8.2 Recommendations

The conclusions of the Certification Body (OCSI) are summarized in sect. 6 (Statement of Certification).

Potential customers of the product "CryptoFlow Net Creator v5.3" are suggested to properly understand the specific purpose of certification reading this Certification Report together with the Security Target [TDS].

The TOE must be used according to the Security Objectives for the operational environment specified in sect. 4.2 of the Security Target [TDS]. It is assumed that, in the operating environment of the TOE, all the assumptions and the organizational security policies described in the [TDS] are respected.

This Certification Report is valid for the TOE in the evaluated configuration; in particular, Annex A – Guidelines for the secure usage of the product includes a number of recommendations relating to delivery, initialization, configuration and secure usage of the product, according to the guidance documentation provided together with the TOE ([DEL], [INST], [SUP], [CFCN], [CEP]).

9 Annex A – Guidelines for the secure usage of the product

This annex provides considerations particularly relevant to the potential customers of the product.

9.1 TOE Delivery

Several procedures are necessary for Certes to maintain security of the TOE during distribution.

Before shipping, some preliminary activities are performed:

- pre-delivery activities for the software, hardware, and documentation components of the TOE shipment;
- TOE labeling, which includes serial numbers, model numbers and logos;
- TOE Packaging.

Certes uses a third-party carrier, typically UPS, FedEx or DHL, to ship TOE packages to customers.

Customers can use shipping and receiving papers to verify the TOE. The shipping label affixed to the package identifies the customer by company name and company address and indicates a specific individual employee of the company for whom the appliance is intended. The packing list can also be checked to make sure that serial numbers (shown as S/N on the list) on each component match up with the ones on the packing list.

During the initial boot process, the hashes for the installed software are automatically checked against the hashes in the signed manifest file delivered to the customer; any modifications to the code or files will result in a rejection code. This verification check happens automatically at boot time and does not require any action on part of the user.

More detail on such a procedure are contained in “Secure Delivery Document” [DEL].

9.2 Installation, initialization and secure usage of the TOE

The CryptoFlow Net Creator 5.3 software will then installed and configured by the end-customer following the defined deployment documentation:

- “CryptoFlow Net Creator 5.3 Installation Guide” [INST]. This manual describes how a System Administrator is to install the TOE.
- “CryptoFlow Net Creator v5.3 Appliances Guidance Documentation Supplement” [SUP]. This document describes the additional instructions necessary for the TOE to be run securely in CC mode.
- “CFNC User Guide v5.3 [CFCN] and “CEP User Guide v5.3” [CEP]. These manuals describe how a System Administrator configures and maintains the TOE as well as how to set up the required security zones that are connected to the TOE.

10 Annex B – Evaluated configuration

The Target of Evaluation (TOE) is the product “CryptoFlow Net Creator v5.3 Software with CEP220, CEP250, CEP300, CEP420, and CEP520 running CEP v5.3 Firmware”, short name “CryptoFlow Net Creator v5.3”, developed by Certes Networks, Inc.

The TOE is identified in the Security Target [TDS] with the version number 5.3. The name and version number uniquely identify the TOE and the set of its subsystems, constituting the evaluated configuration of the TOE, verified by the Evaluators at the time the tests are carried out and to which the results of the evaluation are applied.

For more details, please refer to sect. 1.5 of the Security Target [TDS].

10.1 TOE operational environment

In Table 2 are summarized the components of the operational environment of the TOE to allow its correct working.

For more details, please refer to sect. 1.4.2 and 1.5.1.1 of the Security Target [TDS].

Component	Requirement
Web browsers	One of the following types of Web browsers should be used: • Microsoft Internet Explorer (IE v11+) • Mozilla Firefox (v64+) • Google Chrome (v71+) • Apple Safari (v12+)
OS	CentOS 6.7 (with the current released updates applied)
CPU	Intel Xeon E3-1270 v5, 3.6 GHz
Memory	8 GB
Disk Space	500 GB minimum

Table 2 – TOE operational environment components

11 Annex C – Test activity

This annex describes the task of both the evaluators and the developer in testing activities. For the assurance level EAL4, augmented with ALC_FLR.3, such activities include the following three steps:

- evaluation of the tests performed by the developer in terms of coverage and level of detail;
- execution of independent functional tests by the evaluators;
- execution of penetration tests by the evaluators.

11.1 Test configuration

For the execution of these activities a test environment has been arranged at the LVS site with the support of the developer, which provided the necessary resources.

Before the tests, the software application has been initialized and configured in accordance with the guidance documentation ([INST], [SUP], [CFCN], [CEP]), as indicated in sect. 9.2. After configuration of the TOE the evaluators checked the status and found that the TOE was installed properly, and the needed services were running.

The test environment is the same as the developer used for testing the TSFI.

11.2 Functional tests performed by the developer

11.2.1 Test coverage

The evaluators have examined the test plan presented by the developer and verified the complete coverage of the functional requirements SFR and the TSFIs described in the functional specification.

11.2.2 Test results

The evaluators executed a series of tests, a sample chosen from those described in the test plan presented by the developer, positively verifying the correct behavior of the TSFI and correspondence between expected results and achieved results for each test.

11.3 Functional and independent tests performed by the evaluators

Therefore, the evaluators have designed independent testing to verify the correctness of the TSFI.

The evaluators did not require any special testing tools to check the TSFI selected for independent testing.

In the design of independent tests, the evaluators have considered aspects that in the developer test plan were not present, or ambiguous, or inserted in more complex tests, which covered a mix of interfaces but with a level of detail not adequate.

The evaluators also designed and executed some tests independently from similar tests of the developer, based only on the evaluation documentation.

All independent tests performed by evaluators generated positive results.

11.4 Vulnerability analysis and penetration tests

For the execution of these activities the same test environment already used for the activities of the functional tests has been used (see sect. 11.1)

The evaluators have first verified that the test configurations were consistent with the version of the TOE under evaluation, that is indicated in the [TDS], sect. 1.2.

In a first phase, the evaluators have conducted researches using various sources in the public domain, such as Internet, books, publications, conference proceedings, including the various editions of ICCC, JIL and CCDB documents, etc., in order to identify known vulnerabilities applicable to types of products similar to the TOE. In this research the Linux operating system has been also considered, part of the operational environment, but needed for the correct operation of the TOE. They identified some potential vulnerabilities.

In a second step, the evaluators examined the evaluation documentation (Security Target, functional specification, TOE design, security architecture, operational documentation, site visit report) to identify any additional potential vulnerabilities of the TOE. From this analysis, together with the source code examination, the evaluators have actually determined the presence of other potential vulnerabilities.

The evaluators have analyzed in detail the potential vulnerabilities identified in the two previous steps, to ensure their effective exploitability in the TOE operating environment. This analysis led to identify several actual potential vulnerabilities.

Therefore, the evaluators have designed some possible attack scenarios, with Enhanced-Basic attack potential, and penetration tests to verify the exploitability of the potential candidate vulnerabilities. The penetration tests have been described with sufficient detail for their repeatability using for this purpose test sheets, also used, appropriately compiled with the results, as the report of the tests themselves. The evaluator used some tools (Kali Linux and Burp Suite Pro) for executing the tests.

The execution of the penetration tests confirmed the presence of vulnerabilities potentially exploitable by an attacker with a potential of attack Enhanced-Basic. These results were promptly reported to the Developer, via an Observation Report. The Developer has replied, accepting the evaluators' observations and releasing a new version of the TOE. The evaluators installed such a new version of the TOE in the test environment, and were able to verify that the solutions proposed by the Developer have solved all the problems raised with the previous observations.

On the basis of such results, the evaluators have actually found that no attack scenario with potential Enhanced-Basic can be completed successfully in the operating environment of the TOE as a whole. Therefore, none of the previously identified potential vulnerabilities can be exploited effectively. However, they have identified three residual vulnerabilities, i.e. vulnerabilities that could be exploited only by an attacker with attack potential beyond Enhanced-Basic.