MINISTERIO DE LA PRESIDENCIA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN

REF: 2015-10-INF-1627 v1	Created by: CERT10
Target: Expediente	Revised by: CALIDAD
Date: 12.05.2016	Approved by: TECNICO

CERTIFICATION REPORT

File: 2015-10 NERA

Applicant: RO14664386 Nera Computers S.R.L.

References:

[EXT-2756] Certification request of NERA

[EXT-2989] Evaluation Technical Report of NERA.

The product documentation referenced in the above documents.

Certification report of the product Certus Erasure Engine v3.2, as requested in [EXT-2756] on 01/04/2015, and evaluated by the laboratory Epoche & Espri S.L.U., as detailed in the Evaluation Technical Report [EXT-2989] received on 02/03/2016.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product Certus Erasure Engine v3.2.

Certus Erasure is a software product designed to fulfil the need for protection of the sensitive data stored on computers or storage devices selected for reuse or recycle. It permanently erases from storage devices addressable data such as files, folders, partitions and other user or operating system hidden areas, and in the same time it verifies the result and provides reliable evidence related to success or failure. It is compatible with x86 architecture systems and ATA, SATA, SCSI, SAS, FC, or USB attached storage devices. The following are the erasing standards (patterns) supported by the product: Standard Overwrite, British HMG IS5 Baseline, Russian GOST R 50739-95, NSA 130-2, British HMG IS5 Enhanced, US DoD 5220.22-M, NCSC-TG-025, Navso P-5329-26, US Air Force 5020, Bruce Schneier, Canadian OPS-II, German VSITR, Gutmann Algorithm.

The Target of Security (TOE) evaluated is Certus Erasure Engine (CEE) module. It represents only a part of the whole software product Certus Erasure. This module (CEE) is responsible for:

- data erasing;
- data erase verification;
- audit data collection;
- report data generation and delivery.

Developer/manufacturer: NERA COMPUTERS S.R.L.

Sponsor: NERA COMPUTERS S.R.L.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Epoche & Espri S.L.U.

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL3 + ALC_FLR.1.

Evaluation end date: 02/03/2016.

All the assurance components required by the evaluation level EAL3 (augmented with ALC_FLR.1) have been assigned a “PASS” verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the “PASS” verdict to the whole evaluation due all the evaluator actions are satisfied for the EAL3 + ALC_FLR.1, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

Considering the obtained evidences during the instruction of the certification request of the product Certus Erasure Engine v3.2, a positive resolution is proposed.

TOE SUMMARY

The Target of Security (TOE) evaluated is **Certus Erasure Engine** (CEE) module. It represents only a part of the whole software product Certus Erasure. This module (CEE) is responsible for:

- Data erasing.
- Data erase verification.
- Audit data collection.
- Report data generation and delivery.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL3 and the evidences required by the additional component ALC_FLR.1, according to Common Criteria v3.1 R4.

Class	**Family/Component**
ADV Development	ADV_ARC.1 Security architecture description ADV_FSP.3 Security-enforcing functional specification ADV_TDS.2 Basic design
AGD Guidance Documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC Life-Cycle Support	ALC_CMC.3 Use of a CM system ALC_CMS.3 Parts of the TOE CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Development security ALC_FLR.1 Flaw reporting procedures ALC_LCD.1 Life-cycle definition
ASE Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition ASE_INT.1 ST introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE summary specification
ATE Tests	ATE_COV.2 Evidence of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional testing ATE_IND.2 Independent testing - sample
AVA Vulnerability Assessment	AVA_VAN.2 Vulnerability analysis

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria v3.1 R4:

Class	Family/Component
FAU Security Audit	FAU_GEN.1 Data Generation
FDP User Data Protection	FDP_RIP.1 Residual Information Protection
FPT Protection of the TSF	FPT_ITI.1 Integrity of exported TSF data

IDENTIFICATION

Product: Certus Erasure Engine v3.2

Security Target: Security Target Document for Certus Erasure Engine v3.2, Version 1.9, dated February 16, 2016.

Protection Profile: No.

Evaluation Level: Common Criteria v3.1 R4 – EAL3 + ALC_FLR.1.

SECURITY POLICIES

The use of the product Certus Erasure Engine v3.2 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target. In short, it establishes the need of implementing organizational policies related to the following aspects.

Policy 01: P.AUDIT

The TOE will generate audit records containing information pertaining to storage devices erasure process.

Policy 02: P.REPORTS

The TOE will export reports in such manner as their integrity can be verified.

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

Assumption 01: A.COMPETENT_USERS

The users (persons using TOE) are trusted, competent, trained and they are following the software guidance documentation and internal procedures.

Assumption 02: A.BEHAVED_DRIVES

The storage devices targeted to be erased are well behaved, and expose the full storage capability to the operating system.

Assumption 03: A.BIOS_PREVENTING

The BIOS settings that can interfere with the erasing process by preventing the erasure are properly configured (not preventing the process).

Assumption 04: A.SYSTEM_TIME

The system's time is properly set up in the CMOS chip, prior to start the erasure process, as it will be used for the auditing/reporting.

Assumption 05: A.SECURE_LOCATION

The TOE will be used inside a secure location and physical custody will be maintained by an authorised person.

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product Certus Erasure Engine v3.2, although the agents implementing attacks have the attack potential according to the **basic** attack potential of EAL3 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are categorized below.

Threat 01: T.DATA_RECOVERY

An attacker having access to the storage device after the data erasure is able to compromise the confidentiality of the original data stored on it, by recovering the mentioned data.

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are categorized below.

Environment objective 01: OE.COMPETENT_USERS

The users (persons using TOE) will be trusted, competent, trained and they will follow the guidance documentation.

Environment objective 02: OE.BEHAVED_DRIVES

The only storage devices that are going to be erased by the TOE behave as expected and exposes the full storage capability to the operating system.

Environment objective 03: OE.BIOS_PREVENTING

The BIOS settings that can interfere with the erasing process will be properly configured (not preventing the process).

Environment objective 04: OE.SYSTEM_TIME

The operating environment will provide correct system time.

Environment objective 05: OE.SECURE_LOCATION

The location where TOE will be used will be a secure one.

The details of the product operational environment (assumptions, threats and organisational security policies) and the TOE security requirements are included in the associated security target.

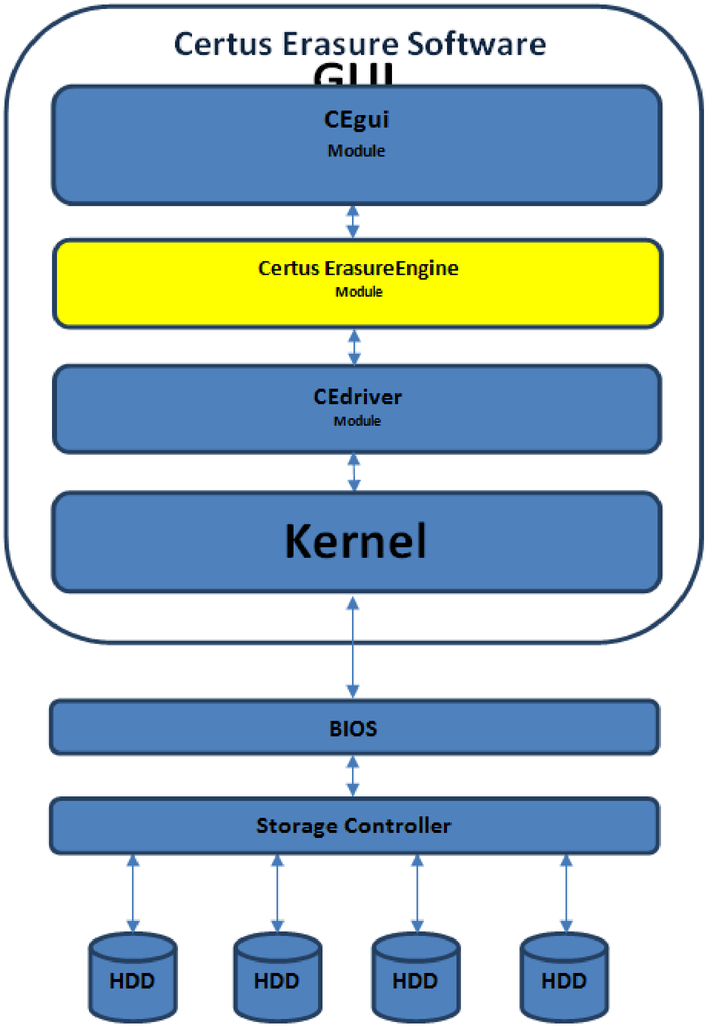
ARCHITECTURE

LOGICAL ARCHITECTURE

After it is initiated by CEgui module, the TOE (CEE module) is executing its designed security functions. In order to erase all addressable data stored on selected device and making impossible any future data recovery on that device, TOE is overwriting the full capacity of the selected drive with the pattern of values corresponding to the selected erasure standard. The supported erasure standards are listed in Table 1-1.

During the process, a verification of the erase is carried out by TOE. It is reading and verifying the values written in the last writing pass requested by the erasure standard. The granularity of verification can be defined by the user (person using TOE).

TOE is also keeping record of all security relevant events and support the user (person using TOE) with information about the storage device identification, erasure standard used for erasing, status of the erasure process, how special areas was handled and what areas could not be erased. A report containing this information is generated at the end of the erasure and it's reliable sent to the CEgui module (using SHA1 digest algorithm for integrity checking).



PHYSICAL ARCHITECTURE

As one of the component module of the Certus Erasure product, the TOE (CEE) is actually a binary file named erasure_engine, residing on the file system created in RAM after booting from the USB Drive containing Certus Erasure software.

The media used for product delivery is a bootable USB drive.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- AGD_OPE.1 Documentation for Certus Erasure Engine, Version 1.3
- AGD_PRE.1 Documentation for Certus Erasure Engine, Version 1.4
- ALC_FLR.1 Documentation for Certus Erasure Engine

PRODUCT TESTING

The developer has executed tests for all the SFRs and TSFIs. All the tests have been performed by the developer in its premises, with a satisfactory result.
During the evaluation process it has been verified each unit test checking that the security functionality that covers has been identified and also that the kind of test is appropriate to the function that is intended to test.

All the tests have been developed using the appropriate testing scenario to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

To verify the results of the developer tests, the evaluator, having available a testing environment equal to the one used during the vendor test phase, has executed all the developer functional tests in the evaluation laboratory. The evaluator has verified that the obtained results are consistent with the results obtained by the developer.

It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product.

EVALUATED CONFIGURATION

The software and hardware requirements, as well as the referenced options are indicated below. Therefore, for the operation of the product Certus Erasure Engine v3.2 it is necessary the disposition of the following software components:

- BIOS (provided by the hardware platform).

Regarding the hardware components, these are the requirements of the hardware platform:

- x86 computer system architecture.
- ATA, SCSI, SATA, SAS, FC, USB hard disk controllers.
- ATA, SCSI, SATA, SAS, FC, USB hard disk drives.

Among all the possibilities offered by these software and hardware requirements, the configuration selected for the evaluation is the following:

Hardware Platform:

Description	**Product**	**Vendor**
Motherboard	P55-GD65 (MS-7583)	Micro-Star International Co. Ltd.
CPU	Intel(R) Core(TM) i7 CPU 860@2.80GHz	Intel Corporation
RAM Memory	DIMM SDRAM Synchronous 1333 MHz (0,8 ns) 4GiB	-
Host Bridge	Core Processor DMI	Intel Corporation
USB Controller	5 Series/3400 Series Chipset USB2	Intel Corporation
Ethernet Interface	RTL8111/8168/8411 PCI Express Gigabit Ethernet Controller	Realtek Semiconductor Co. Ltd.
Serial Attached SCSI Controller	SAS2008 PCI-Express Fusion-MPT SAS-2 [Falcon]	LSI Logic / Symbios Logic
SCSI Storage Controller	53c1030 PCI-X Fusion-MPT Dual Ultra320 SCSI	LSI Logic / Symbios Logic
Fibre Channel	Thor LightPulse Fibre Channel Host Adapter	Emulex Corporation
IDE Interface	5 Series/3400 Series Chipset SATA IDE Controller	Intel Corporation
Video Controller	GF119 [GeForce 510]	NVIDIA Corporation

Storage devices:

Vendor	**Model**	**Serial**	**Firmware**	**User addressable sectors**	**Sect. size**	**Interf. type**
Seagate	ST336754SS	3KQ285ZF	S411	71132959	512	SAS
Seagate	ST920217AS	5PW2VKSC	3.01	39070080	512	SATA
Hitachi	HCC543216A7A380	ES1OA60W	ES1OA60W	312581808	512	SATA
Western Digital	WDC WD1600AABS-56PRA0	WD-WMAP96372543	05.06H05	312581808	512	SATA
Seagate	ST336607LW	3JA7B087	DS09	71132959	512	SCSI
Samsung	HM321HX	C4371G82AA6CFL	2AJ10001	625142448	512	USB
HP	BD07255B29	3HZ1BSMV	HP05	143374738	512	FC
HP	BD07254498	3EK20TCD	3BE9	142264000	512	FC

EVALUATION RESULTS

The product Certus Erasure Engine v3.2 has been evaluated against the Security Target "Security Target Document for Certus Erasure Engine v3.2, Version 1.9, dated February 16, 2016".

All the assurance components required by the evaluation level EAL3 + ALC_FLR.1 have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "**PASS**" **verdict** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL3 + ALC_FLR.1, as defined by the Common Criteria v3.1 R4 and the CEM v3.1 R4.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

The fulfilment of the assumptions indicated in the security target is a key point as it implies TOE environment configurations that leave some potential vulnerabilities out of the scope.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product Certus Erasure Engine v3.2, a positive resolution is proposed.

GLOSSARY

ATA	AT Attachment. Also known as Parallel ATA (PATA)
BIOS	Basic Input Output System
CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FC	Fibre Channel
OC	Organismo de Certificación (*Certification Body*)
SAS	Serial Attached SCSI
SATA	Serial ATA

SCSI	Small Computer System Interface
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
USB	Universal Serial Bus

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R4, September 2012.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R4, September 2012.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R4, September 2012.

SECURITY TARGET

Along with this certification report, the complete security target of the evaluation is available in the Certification Body: “Security Target Document for Certus Erasure Engine v3.2, Version 1.9, dated February 16, 2016”.