CertusErasure
SOFTWARE

Common Criteria Security Target

for

Certus ErasureEngine

Document Version: 1.9

Date: 16.02.2016

1- Security Target Introduction

1.1 -ST Reference

1.1.1 - ST Identification

Security Target Document for Certus Erasure Engine v3.2

1.1.2 - ST Version

1.9

1.1.3 - ST Date

February 16, 2016

1.2 - TOE Reference

1.2.1 - TOE Identification

Certus ErasureEngine

1.2.2 - TOE Version

v3.2

1.3 - Product Overview

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:

Erasing Standard	**Description**
Standard Overwrite	Single pass over each sector writing 0x00.
British HMG IS5 Baseline	Pass over each sector once writing random value.
Russian GOST R 50739-95	Pass over each sector 2 times writing 0x00anda random value.
NSA 130-2	Pass over each sector 2 times writing a random value.
British HMG IS5 Enhanced	Pass over each sector 3 times writing 0x00, 0xFF and a random value.
US DoD 5220.22-M	Pass over each sector 3 times writing 0x00, 0xFF and a random value.
NCSC-TG-025	Pass over each sector 3 times writing 0x00, 0xFF and a random value.
Navso P-5329-26	Pass over each sector 3 times writing 0x00, 0xFF and a random value.

US Air Force 5020	Pass over each sector 3 times writing0xFF, 0x00 and a random value.
Bruce Schneier	Pass over each sector 7 times, writing 0xFF, 0x00 and then five times random values.
Canadian OPS-II	Pass over each sector 7 times writing0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF and a random value.
German VSITR	Pass over each sector 7 times writing0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF and 0xAA.
Gutmann Algorithm	Pass over each sector 35 times, writing random values the first four times, then respectively write 0x555555, 0xAAAAAA, 0x924924, 0x492492, 0x249249, 0x000000, 0x111111, 0x222222, 0x333333, 0x444444, 0x555555, 0x666666, 0x777777, 0x888888, 0x999999, 0xAAAAAA, 0xBBBBBB, 0xCCCCCC, 0xDDDDDD, 0xEEEEEE, 0xFFFFFF, 0x924924, 0x492492, 0x249249, 0x6DB6DB, 0xB6DB6D, 0xDB6DB6 and another four times random values.

Table 1-1: Supported Erasing Standards

1.4 - TOE Overview

The Target of Security (TOE) evaluated in this Security Target 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;
- reportdata generation and delivery.

1.4.1 – Product Security Features not included in the TOE

Certus Erasure implements the following security features that are out of the TOE:

- secure connection to the remote management platform;
- authentication and authorisation to the remote management platform.

All these security features are out of the scope of the evaluation, and therefore no assurance level is associated to them.

The following software and hardware components are required for the TOE functioning. These are not part of the TOE, and therefore are not evaluated and no assurance level is associated to them.

1.4.2 – Non-TOESoftware and Hardware

Non-TOE software components:

- **BIOS**;
- **Kernel** module;
- **CEdriver** module;

- **CEgui** module;

Non-TOE hardware components:

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

1.5 - TOE Description

1.5.1 Evaluated Configuration

The following configuration has been used for evaluation:

Hard Disk Drives						
Vendor	**Model**	**Serial**	**Firmware**	**User addressable sectors**	**Sector size**	**Interface 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

Erasure Standard
Standard Overwrite (Single pass over each sector writing 0x00)

Physical Machine(x86 computer system)		
Description	**Product**	**Vendor**
Motherboard	P55-GD65 (MS-7583)	MICRO-STAR INTERNATIONAL CO.LTD.
CPU	Intel(R) Core(TM) i7 CPU860@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

Fibre Channel Hard Drive Enclosure
HP Storageworks DS-MG521-AA

1.5.2 TOE Physical Scope

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.

The guidance is delivered together with the product on separate media support as PDF document, in order to support the user with proper operation information. It is also available for download, on support webpage:

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

1.5.3 TOE Logical Scope

After it is initiated by CEgui module, the TOE(CEE module) is executing itsdesigned 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 alsokeeping 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 digestalgorithm for integrity checking).

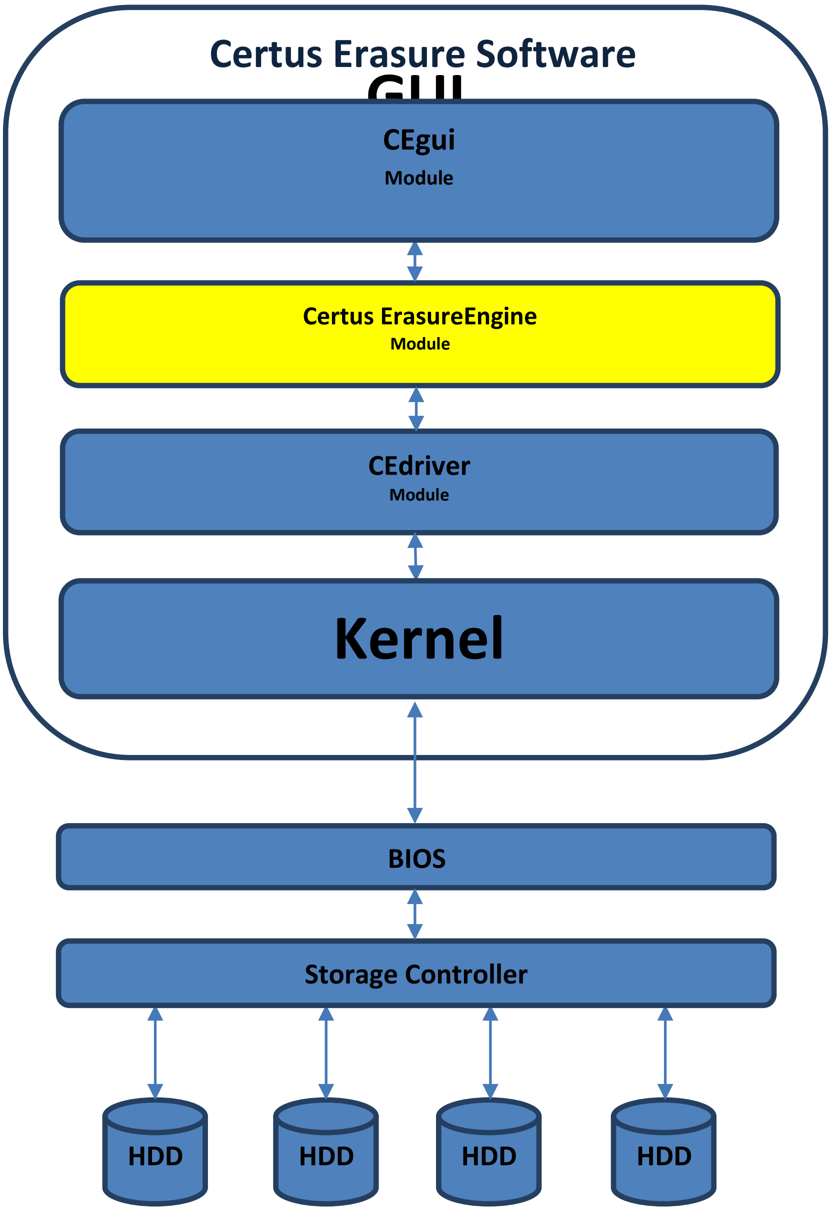

Image1-1: TOE and the other components of Certus Erasure

2 - Conformance Claims

2.1 - CC Version Conformance

This TOE is conforming to the Common Criteria for Information Technology Security, Version 3.1, Revision 4, September 2012.

2.2 - CC Part 2 Conformance

This Security Target is CC Part 2 conformant.

2.3 - CC Part 3 Conformance

This Security Target is CC Part 3 conformant.

2.4 - Protection Profile Conformance

This Security Target (ST) has no Protection Profile (PP) to conform with.

2.5-Security Requirement Packages Conformance

This TOE is package-augmented EAL3 + ALC_FLR.1 conformant.

2.6 - Conformance Claim Rationale

This Security Target (ST) has no conformance claim rationale.

3 - Security Problem Definition

3.1 -Threats

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.

3.2 - Organization Security Policies (OSP)

P.AUDIT

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

P.REPORTS

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

3.3 -Assumptions

3.3.1 - Personnel Assumptions

A.COMPETENT_USERS

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

3.3.2 - System Assumptions

A.BEHAVED_DRIVES

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

A.BIOS_PREVENTING

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

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.

3.3.3 - Environment Assumptions

A.SECURE_LOCATION

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

4 - Security Objectives

4.1 - Security Objectives for the TOE

The following security objectives are to be satisfied by the TOE:

O.PROPER_ERASE

The TOE shall be able to erase all addressable data stored on selected storage device, making impossible any future data recovery on that device.

O.PROPER_AUDIT

The TOE shall provide means for security relevant events recording and supporting the user (person using TOE) with information about erasure standard, the status of the erasure, special area handling and areas that could not be erased.

O.PROPER_REPORTS

The TOE shall export reports containing information about the erasure process, guarantying the integrity of the data exported.

4.2 - Security Objectives for the Operational Environment

The following security objectives are to be satisfied by the operational environment:

OE.COMPETENT_USERS

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

OE.BEHAVED_DRIVES

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

OE.BIOS_PREVENTING

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

OE.SYSTEM_TIME

The operating environment will provide correct system time.

OE.SECURE_LOCATION

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

4.3 - Security Objectives Rationale

This section will provide the evidence on how Security Objectives will counter all Threats, enforce OSP and upheld Assumptions. The mapping exposed in the following table, will be further explained in more detailed rationale.

	O.PROPER_ERASE	O.PROPER_AUDIT	O.PROPER_REPORTS	OE.COMPETENT_USERS	OE.BEHAVED_DRIVES	OE.BIOS_PREVENTING	OE.SYSTEM_TIME	OE.SECURE_LOCATION
T.DATA_RECOVERY	X							
P.AUDIT		X						
P.REPORTS			X					
A.COMPETENT_USERS				X				
A.BEHAVED_DRIVES					X			
A.BIOS_PREVENTING						X		
A.SYSTEM_TIME							X	
A.SECURE_LOCATION								X

Table 4-1: Security Objectives mapping against Threats, SPO and Assumptions

Threat Name	**T.DATA_RECOVERY**	
Threat Description	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.	

TOE Security Objective Name	O.PROPER_ERASE	
TOE Security Objective Description	The TOE shall be able to erase all addressable data stored on selected storage device, making impossible any future data recovery on that device.	
Security Objectives Rationale	The threat T.DATA_RECOVERY is countered by TOE security objective O.PROPER_ERASE. TOE security objective O.PROPER_ERASE ensures that the TOE will overwrite completely the content of the specified storage device.	

Organizational Security Policy Name	**P.AUDIT**
Organizational Security Policy Description	The TOE will generate audit records containing information pertaining to storage devices erasure process.
TOE Security Objective Name	O.PROPER_AUDIT
TOE Security Objective Description	The TOE shall provide means for security relevant events recording and supporting the user (person using TOE) with information about erasure standard, the status of the erasure, special area handling and areas that could not be erased.
Security Objectives Rationale	The OSP P.AUDIT is enforced by TOE security objective O.PROPER_AUDIT. TOE security objective O.PROPER_AUDIT, ensures that specified security relevant events will be recorded in order to monitor the whole process.

Organizational Security Policy Name	**P.REPORTS**
Organizational Security Policy Description	The TOE will export reports in such manner as their integrity can be verified.
TOE Security Objective Name	O.PROPER_REPORTS

TOE Security Objective Description	The TOE shall export reports containing information about the erasure process, guarantying the integrity of the data exported.
Security ObjectiveRationale	The OSP P.REPORTS is enforced by TOE security objective O.PROPER_REPORTS. This will ensure that all data collected by the audit component will be exported and will use an integrity checking mechanism to ensure exported data integrity.

Assumption Name	**A.COMPETENT_USERS**
Assumption Description	The users (persons using TOE) are trusted, competent, trained and they are following the software guidance documentation and internal procedures.
Environment Security Objective Name	OE.COMPETENT_USERS
Environment Security Objective Description	The users (persons using TOE) will be trusted, competent, trained and they will follow the guidance documentation.
Security Objectives Rationale	The assumption A.COMPETENT_USERS is upheld by environment security objective OE.COMPETENT_USERS. This ensures that only trusted, competent and trained users (persons using TOE) will operate TOEas per provided guidance documentation.

Assumption Name	**A.BEHAVED_DRIVES**
Assumption Description	The storage devices targeted to be erased are well behaved, and expose the full storage capability to the operating system.
Environment Security Objective Name	OE.BEHAVED_DRIVES
Environment Security Objective Description	The only storage devices that are going to be erased by the TOE behave as expected and expose the full storage capability to the operating system.
Security Objectives Rationale	The assumption A.BEHAVED_DRIVES is upheld by environment security objectives OE.BEHAVED_DRIVES. This ensures that storage devices targeted to be erased will be well behaved and

	expose the full storage capability to the operating system.

Assumption Name	**A.BIOS_PREVENTING**
Assumption Description	The BIOS settings that can interfere with the erasing process by preventing the erasure are properly configured (not preventing the process).
Environment Security Objective Name	OE.BIOS_PREVENTING
Environment Security Objective Description	The BIOS settings that can interfere with the erasing process will be properly configured (not preventing the process).
Security Objectives Rationale	The assumption A.BIOS_PREVENTING is upheld by environment security objective OE.BIOS_PREVENTING. This ensures that the BIOS settings that can interfere with the erasing process will be properly configured by the users (persons using TOE) in such a way to not prevent the process.

Assumption Name	**A.SYSTEM_TIME**
Assumption Description	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.
Environment Security Objective Name	OE.SYSTEM_TIME
Environment Security Objective Description	The operating environment will provide correct system time.
Security Objectives Rationale	The assumption A.SYSTEM_TIME is upheld by environment security objective OE.SYSTEM_TIME. This ensures that the system's time will be properly set up in the CMOS chip by the user (person using TOE), prior to start the erasure, and the audit component will obtain reliable timestamps.

Assumption Name	**A.SECURE_LOCATION**
Assumption	The TOE will be used into a secure location and physical custody will be maintained

Description	by an authorised person.
Environment Security Objective Name	OE.SECURE_LOCATION
Environment Security Objective Description	The location where TOE will be used will be a secure one.
Security Objective Rationale	The assumption A.SECURE_LOCATION is upheld by environment security objective OE.SECURE_LOCATION. This will ensure that the TOE will be used only in controlled access areas and physical custody will be maintained by an authorised person.

5 - Security Requirements

5.1 - Security Functional Requirements

SFR #1		
Security Functional Class	FDP	User Data Protection
Security Functional Family	FDP_RIP.1	Subset residual information protection
		Hierarchical to:No other components
		Dependencies:No dependencies
Security Functional Component	FDP_RIP.1.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: **deallocation of resources from**] the following objects: [assignment: **storage device**].

SFR #2		
Security Functional Class	FAU	Security Audit
Security Functional Family	FAU_GEN.1	Audit data generation
		Hierarchical to: No other components
		Dependencies: FPT_STM.1 - Reliable Time Stamps
Security Functional Component	FAU_GEN.1.1	The TSF shall be able to generate an audit record of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [selection: **not specified**] level of audit; and

		c) [assignment:**erasure process events**].
Security Functional Component	FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of the event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: **TOE identification, system identification, disk identification, internal id, model info, manufacturer info, total number of sectors, sector size, overwrite pattern, verify percentage, number of sector read/write failures, date and time operation was started, date and time operation was completed**].

SFR #3		
Security Functional Class	FPT_ITI.1	Protection of the TSF
Security Functional Family	FPT_ITI.1	Integrity of exported TSF data
		Hierarchical to: No other components
		Dependencies:No dependencies
Security Functional Component	FPT_ITI.1.1	The TSF shall provide the capability to detect modifications of all TSF data during transmission between the TSF and another trusted IT product within the following metric [assignment: **SHA1 digest**].
Security Functional Component	FPT_ITI.1.2	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [assignment: **exit of program**] if modifications are detected.

5.2 - Security Assurance Requirements

EAL3 (methodically tested and checked) package augmented with ALC_FLR.1 component is the assurance level claimed for the TOE. The ALC_FLR.1 component is adding assurance for systematic flaw remediation.

REQUIREMENT CLASS	REQUIREMENT COMPONENT	
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design

AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative Procedures
ALC: Life-cycle support	ALC_CMC.3	Authorisation controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
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	Analysis 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

Table 5-1: EAL3 augmented with ALC_FLR.1 assurance requirements

5.3 - Security Functional Requirements Rationale:

This section will provide evidence on how all Security Objectives are satisfied by theappropriate Security Functional Requirements (SFR).The mapping exposed in the following table, will be further explained in more detailed rationale.

	Audit data generation	Subset residual information protection	Integrity of exported TSF data
	FAU_GEN.1	FDP_RIP.1	FPT_ITI.1
O.PROPER_AUDIT	X		
O.PROPER_ERASE		X	
O.PROPER_REPORTS			X

Table 5-2: Mapping of Security Objectives against Security Functional Requirements

Security Objective	**O.PROPER_AUDIT**
Security Objective Description	The TOE shall provide means for security relevant events recording and supporting the user (person using TOE) with information about erasure standard, the status of the erasure, special area handling and areas that could not be erased.
TOE Security Functional Requirement	FAU_GEN.1
TOE Security Functional Requirement Description	Audit data generation. Audit data generation defines the level of auditable events, andspecifies the list of data that shall be recorded in each record.
Security Functional Requirement Rationale	The TOE security objective O.PROPER_AUDITis enforced by TOE security functional requirement FAU_GEN.1. TOE SFR FAU_GEN.1 ensures that the security objective O.PROPER_AUDIT is satisfied by requiring TSFtodefine the level of auditable events and clearly specifying the security relevant events that will be recorded.

Security Objective	**O.PROPER_ERASE**
Security Objective Description	The TOE shall be able to erase all addressable data stored on selected storage device, making impossible any future data recovery on that device.
TOE Security Functional Requirement	FDP_RIP.1
TOE Security Functional Requirement Description	Subset residual information protection requires that the TSFensure that any residual information content of any resources is unavailableto a defined subset of the objects controlled by the TSF upon the resource'sallocation or deallocation.
Security Functional Requirement Rationale	The TOE security objective O.PROPER_ERASE is enforced by TOE security functional requirement FDP_RIP.1. TOE SFR FDP_RIP.1 ensures that the security objective O.PROPER_ERASE is satisfied by requiring TSF that any residual information content from the resource (original user data) will be made unavailable at deallocation of the resource from the targeted storage device.

Security Objective	**O.PROPER_REPORTS**
Security Objective Description	The TOE will export reports in such manner as their integrity can be verified.
TOE Security Functional Requirement	FPT_ITI.1
TOE Security Functional Requirement Description	Integrity of exported TSF data. Inter-TSF detection of modification provides the ability to detectmodification of TSF data during transmission between the TSF and anothertrusted IT product, under the assumption that another trusted IT product iscognisant of the mechanism used.
Security Functional Requirement Rationale	The TOE security objective O.PROPER_REPORTS is enforced by TOE security functional requirement FPT_ITI.1. TOE SFR FPT_ITI.1 ensures that the security objective O.PROPER_REPORTS is satisfied by requiring TSFto provide the capability to detect modification of all TSFdata during report transmission, using SHA1 digest. It also performs the assignment of terminating the application when integrity modification is detected.

5.4 - Security Functional Requirements Components Dependencies Rationale

This section describes how security functional requirements component dependencies are satisfied and the corresponding rationale.

Security Functional Requirements	**Dependencies**	**Rationale**
FDP_RIP.1 (Subset residual information protection)	None	None
FAU_GEN.1 (Audit data generation)	FPT_STM.1 (Time Stamps)	Not satisfied by TOE. Date and time is provided by TOE environment (OE.PROPER_TIME).
FPT_ITI.1 (Integrity of exported TSF data)	None	None

Table 5-3: SFR Components Dependencies Rationale

5.5 - Security Assurance Requirements Rationale

EAL3 evaluation assurance level augmented with ALC_FLR.1 (EAL3+ALC_FLR.1) has been chosen in order to comply with market exigencies for this typology of products as it provides to the customers a comfortable level of assurance that is consistent with today’s good practices.

6 - TOE Summary Specification

This section identifies the Security Functions provided by the TOE, mapped to the Security Functional Requirements contained in this Security Target (ST).

Security Functions	Security Functional Requirements
SF.PROCESS_CONTROLLER	FAU_GEN.1 - Audit data generation
	FPT_ITI.1 - Integrity of exported TSF data
SF.DATA_ERASER	FDP_RIP.1 - Subset residual information protection

Table 6-1: Mapping of Security Functions against Security Functional Requirements

6.1 – SF.PROCESS_CONTROLLER

The SF.PROCESS_CONTROLLER function of the TOE enforces the FAU_GEN.1 and FPT_ITI.1 requirements.

FAU_GEN.1 requires a reliable timestamp, which is provided by the Operating System bundled on the TOE bootable USB Drive. The correct date and time information is taken by Operating System from the BIOS at the booting time. Audit data is generated every time when scanning, probing and wiping data storage devices. The output of these actions are sent to the console and in the same time stored by the TOE. Along with the success or failure of events being recorded, the TSF records also info about TOE identification, disk identification, overwrite pattern, number of passes and write failures, date and time when the operation was started, date and time when the operation was completed. Audit data is also generated for the start-up and shutdown of audit. The audit functions available to the user (person using TOE) cannot be disabled and are run automatically.

During and after erasing process, the TOE is verifying the conformity of the erasure process results and the reporting data collected is evaluated for modification during transmission as per FPT_ITI.1 security functional requirement,by SHA1 digest and the program is ended if any integrity issue is found. The TOE user can select the level of erase verification (full verification or partial verification). During the erase verification process, if any nonconformity is detected, the TOE will report that erasure process has failed and the storage device has not been fully erased.

6.2 – SF.DATA_ERASER

This security function is coming to fulfil the requirements of FDP_RIP.1 security functionality. TOE erases existing data by overwriting it (in the evaluated configuration) with the Standard Overwrite pattern(single pass over each sector writing 0x00). Before this, TOE removes Host Protected Area (HPA) and Device Configuration Overlay (DCO). Overwriting operation consists in sequential steps of write and verify data values.

7 – Abbreviations & Terms

The following is the description of the abbreviations and terms used in this Security Target document:

Abbreviation	**Description**
ATA	AT Attachment is an interface standard for the connection of the devices to a host computer.
BIOS	Basic Input / Output System.
DCO	Device Configuration Overlay is an optional feature set for ATA hard drives. It enables the possibility to disable the user or operating system access to certain part of the hard drive. The DCO settings are accessed and controlled with special tools (operating on low level).
FC	Fibre Channel is a high-speed network technology (2, 4, 8 and 16gigabit per second rates) primarily used to connect computer data storage.
GUI	Graphical User Interface.
HPA	Host Protected Area is an area of a hard drive that is not normally visible to an operating system.
IDE	Integrated Drive Electronics is an interface standard for the connection of storage devices such as hard disk drives to a host computer.
Kernel	The central component for most Operating Systems that is primarily responsible for starting and stopping programs, handling the file system, as well as other low level tasks most programs share.
SAS	Serial ATA computer bus is a storage interface for connecting host bus adapters to storage devices.
SCSI	Small Computer System Interface is a set of standards for physically connecting and transferring data between computers and peripheral devices.
USB	Universal Serial Bus is a serial bus standard to connect devices to a host computer.

Table 7-1: Abbreviations& Terms