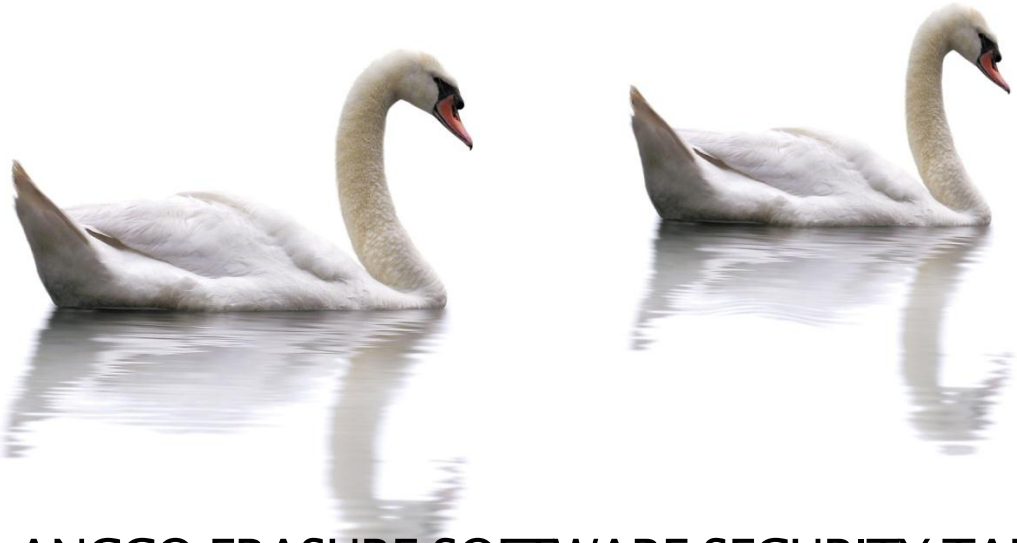
blancco



BLANCCO ERASURE SOFTWARE SECURITY TARGET

Security Target Document for the Common Criteria Certification of Blancco Erasure Software v5.1.0 for X86 architecture

Version 5.0
ID 96

13.12. 2011
Juha Levo, Quality Manager

TABLE OF CONTENTS

LIST OF TABLES

SECURITY TARGET INTRODUCTION

Abbreviations and Terms

This ST uses following abbreviations and terms.

Table 1. Abbreviations and Terms

APPREVIATION AND TERMS	DESCRIPTIONS
ATA	AT Attachment (ATA), is an interface standard for the connection of storage devices such as hard disks
BES	Blancco Erasure Software
BEM	Blancco Erasure Module
DCO	Device Configuration Overlay (DCO), 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 a low level
Fibre Channel	Fibre Channel (FC), is a gigabit-speed network technology primarily used for storage networking
FireWire	The IEEE 1394 interface (FireWire), is a serial bus interface standard for high-speed communications and isochronous real-time data transfer, frequently used by personal computers
HPA	Host Protected Area sometimes referred to Hidden Protected Area is an area of a hard drive that is not normally visible to an operating system (OS).
IDE	Integrated Drive Electronics (IDE), is an interface standard for the connection of storage devices such as hard disks
TSF	TOE Security Functionality
RAID	Redundant Array of Inexpensive Disks (RAID), a technology that allowed computer users to achieve high levels of storage reliability from low-cost and less reliable PC-class disk-drive components, via the technique of arranging the devices into arrays for redundancy
SAS	Serial Attached SCSI
SATA	Serial ATA (SATA), computer bus is a storage-interface for connecting host bus adapters to storage devices
SCSI	Small Computer System Interface (SCSI), is a set of standards for physically connecting and transferring data between computers and peripheral devices
USB	Universal Serial Bus (USB) is a serial bus standard to connect devices to a host computer

ST Reference

ST Title – Blancco Erasure Software Security Target

ST Reference – Security Target for Albus v5.1.0

ST Version – 5.0

ST Date – 13th of December 2011

TOE Reference

TOE Identification – Blancco Erasure Module of BES for X86 architecture

TOE Version – 5.1.0

TOE Overview

Blancco Erasure Software (BES) is a solution for end of life management of computer assets. BES is a software product for which different variations are available across a variety of operating systems and hardware platforms such as Intel and SPARC, PC computers and enterprise servers. This Security Target has been written for BES designed and implemented for X86 architecture.

Blancco Erasure Software has modular structure. One of the main modules is called erasure module and it is responsible of the security functions described in this document. Different modules and they responsibilities are described in more detailed manner in TOE Description. Blancco Erasure Module of BES for X86 architecture is the Target of Evaluation

The main function of the BES is to perform hardware detection on a host computer, to display a list of available storage device(s) to the user, and to erase the selected target devices according to a chosen erasure standard. The software also prepares an erasure report after the erasure has finished. This report contains the detailed information about the erasure process, including timing information and a list of problems encountered during the erasure.

BES supports the following storage device connection technologies:

- ATA
- SCSI
- SATA
- SAS
- USB
- FireWire
- Fiber Channel
    - For the TOE, the Fiber Channel provides a point to point access from the TOE to the devices to be erased without network consideration

The storage device type taken into account for this evaluation is Hard Disk Drive (HDD).

Erasure is carried out according to existing standards, or the user may define his own erasure pattern and phases. Table 2 contains a selection of some erasure standards available in the BES:

Table 2. Examples of erasure standards

NAME OF STANDARD	OVERWRITING ROUNDS	OVERWRITING PATTERNS (DIFFERENT ROUNDS SEPARATED WITH COMMA)	SPECIAL REQUIREMENTS
HMG Infosec Standard 5, Lower Standard	1	0x00	Verification is optional
HMG Infosec Standard 5, Higher Standard	3	0x00, 0x55, Random Character	Verification is mandatory
DoD 5220.22-M	3	0x55, 0xAA, Random Character	Verification is mandatory
German Standard BSI/VSITR	7	0x00, 0xFF, 0x00, 0xFF, 0x00, 0xFF, Random Character	

An erasure consists of overwriting normal device areas with predefined or random data, dealing with special device features such as reallocated sectors or HPA/DCO, and partial or full verification of the correctness of erasure process. If the erasure process succeeds, data destruction on the selected storage device areas is 100% guaranteed, and also Secure Erase command can be performed to ATA connected storage devices. Otherwise, failure is reported.

The TOE detects the complete capacity of a device and carries out the erasure process according to the user's settings from all addressable areas of the storage devices as well as from special areas such as:

- DCO
- HPA
- Reallocated Sectors

The TOE is also responsible for the partial or full verification of erasure. If verification of the erasure process indicates that the erasure process has not been performed successfully, TOE will report failure of the erasure.

In its default configuration BES is capable of handling erasure of the storage devices implemented fully or partially according to ATA or SCSI specifications as well as virtual volumes (e.g. disk partitions, RAID volumes) residing in the aforementioned storage devices.

TOE Description

The TOE (Blancco Erasure Module of BES for X86 architecture) is one of the constituent modules of the BES for x86 architecture. The BES is a software product built for the purpose of erasing sensitive data from storage devices under user supervision. Modular structure and consistent inter-modular communication protocol of the product enable it to operate successfully on a number of hardware and software platforms. While implementation details of other BES modules may vary depending on target hardware and software platform, the implementation and main function of the

erasure module remain unchangeable. This guarantees the same robust and secure data erasure process across multiple platforms.

Main functions of the TOE are to handle the erasure process executed on selected storage devices in accordance with the user's configuration settings and to generate a set of data describing the erasure status. Configuration settings define the standard to be applied during the erasure process and the region of the disk that is to be erased.

The erasure process is a multi-step procedure. For each device the following steps are executed:

- Validation and acceptance of the device that is to be erased
- Detection of the full device capacity including protected disk regions
- Detection of disk blocks that cannot be accessed using normal I/O commands
- Overwriting the selected disk region one or more times with a pre-defined or random pattern
- Partial or full verification that the data has truly been erased
- Generation of the output data that is to be used for generating the erasure report

As its input data, erasure module receives a list of data storage devices to process with corresponding erasure standards.

Erasure process results in a data set generated for each device. This includes:

- Total number of data blocks located in the directly accessible area, detected before the erasure process
- Total number of data blocks located in the directly accessible area, detected after the erasure process
- Total number of data blocks located out of the directly accessible area and detected before the erasure process
- Total number of data blocks located out of the directly accessible area and detected after the erasure process
- Total number of data blocks detected in the device, a sum of both directly and indirectly accessible ones, calculated before the erasure process
- Total number of data blocks detected in the device, a sum of both directly and indirectly accessible ones, calculated after the erasure process
- Size of a single data block, given in bytes
- Status of the erasure standard applied
  - Name of the erasure standard;
  - Total number of the unique data blocks processed
  - Erasure standard status
  - Additional information
  - A list of the errors occurred
    - Name of the error
    - Error description
    - Additional info
  - A list of the steps performed
    - Name of the operation/step (e.g. Write, Read, Verify etc.)
    - Description of the operation
    - Total number of the unique data blocks processed
    - Status of the operation
    - Additional information
    - A list of the errors occurred
- A list of the inaccessible areas detected

        - Name of the area
        - Size of the area detected before the erasure process, given in data blocks
        - Size of the area detected after the erasure process, given in data blocks
        - Number of the unique data blocks erased
    - A list of the errors occurred

This information is sufficient for the user to conclude whether erasure process sanitized all the storage device areas specified. This information also tells if storage device areas that were not meant for data destruction have been involved.

In order to successfully fulfill its function, erasure module should operate together with other parts of BES products.

A minimal BES product is a bundle of the following entities:

- Services Module
- Configuration Module
- Detection Module
- Drivers Module
- Erasure Module

In addition TOE requires operating system compatible of the hardware in question. Usually Blancco Ltd. delivers compatible operating system together with the TOE.

The Services Module contains the operations that BES can perform exposed as HTTP Restful Services.

The Configuration Module is in charge of managing different dependencies between modules and options such like erasure standards, available operations etc. It is the first module to run, during the boot phase.

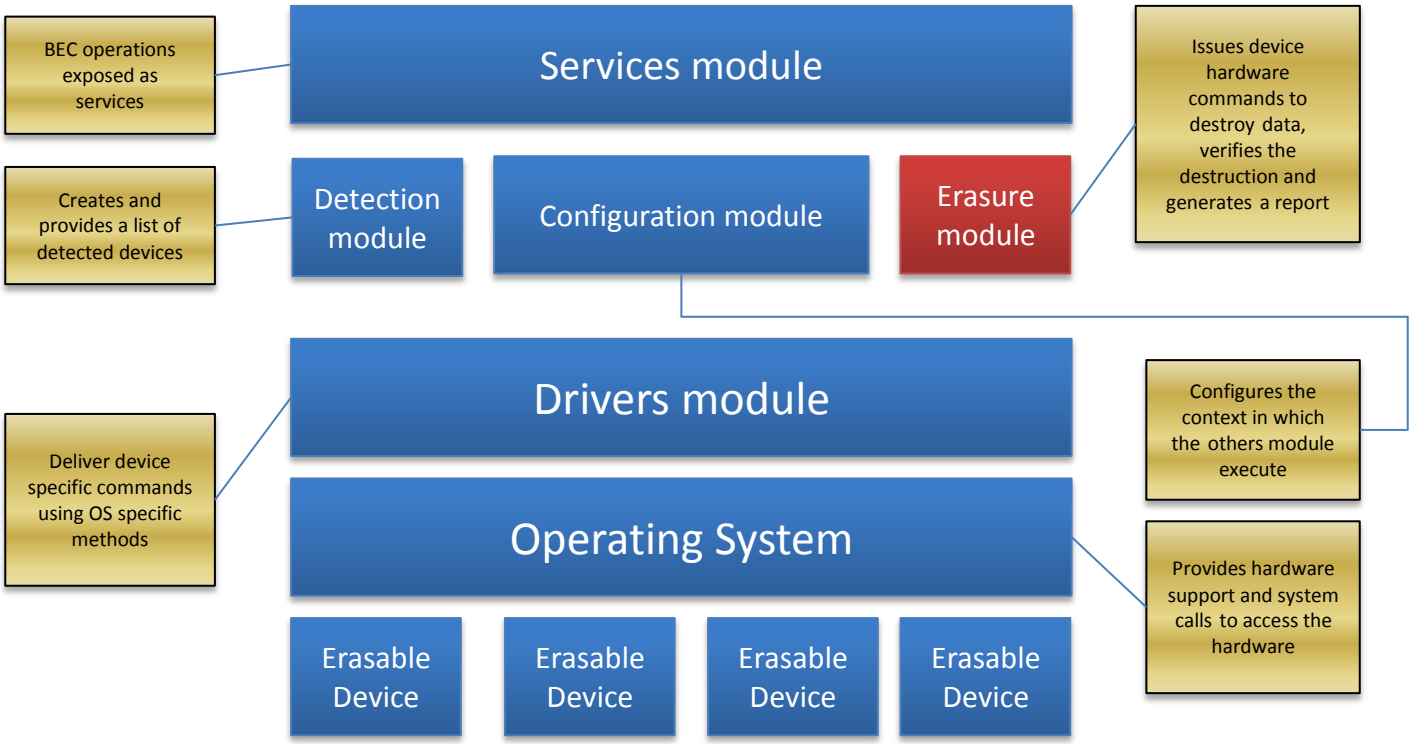
The Detection Module handles the detection of the hardware components on the system it runs. This module constructs the in-memory representation of the system's devices.

The Drivers Module contains the logic for delivering device commands to the devices using OS system calls.

The Erasure Module (the TOE) contains the logic to destroy data on the erasable devices. It fetches the erasure standards description from the Configuration Module and applies the erasure logic to the erasable devices that were detected by the Detection Module. The erasure logic consists in emitting the proper command to the Driver Module. These commands are meant for overwriting the device's area with constant and random data, destroying special device areas and verify the erasure process (partial and full).

In addition BES requires operating system compatible of the hardware in question. Usually Blancco Ltd. delivers compatible operating system together with the BES.

Table 3. The TOE and the other modules of BES



CONFORMANCE CLAIMS

CC Conformance Claim

This TOE is conformant to the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1, Revision 3, July 2009.
  - Part 2 Conformant
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Components, Version 3.1, Revision 3, July 2009.
  - Part 3 Conformant
  - EAL 3 augmented with ALC_FLR.3.

PP Claim

There are no Protection Profiles to which this ST is conformant.

SECURITY PROBLEM DEFINITION

Threats

T.Incomplete_overwrite

TOE fails to overwrite content of the storage devices or a specified part of the storage devices has not been overwritten, and consumer data can still be found.

T.Incorrect_reporting

TOE fails to report correctly about the result of erasure process and/or the capacity of the storage device.

T.Incorrect_parameter_usage

TOE fails to perform erasure as set in configuration parameters, which are given to TOE. With configuration parameters user can select following:

- Erasure standard
- Storage device(s) and partitions to be erased

Assumptions

Personnel Assumptions

A.Competent_users

The persons using the TOE are trusted, trained, competent and follow the application guidance documentation.

A.Proper_procedures

The persons using the TOE must have knowledge and proper procedures in order to modify HW to be erased in order to proper detection of storage devices.

System Assumptions

A.BIOS_modifications

BIOS settings of the HW to be erased must be modified in such way, that they do not prevent the erasure of storage devices.

A.System_clock

BIOS clock of the HW to be erased must be set to the correct time and date for reporting purposes.

SECURITY OBJECTIVES

Security Objectives for the TOE

O.Erasure_process

The TOE is capable to erase all addressable data from the storage devices and partitions selected to be erased, in such way that attempting to read original data from the storage devices will fail.

O.Reporting_content

The TOE shall provide information of the erasure process, consisting of; erasure success or failure, special area handling, erasure standard and information about areas, which could not be erased.

O.Verification_of_erasure

The TOE shall perform verification of the erasure process and report the result of the erasure process.

O.Detection_of_storage_device_capacity

The TOE shall detect the correct capacity of the storage device in order to perform erasure process in secure way

Security Objectives for the Operational Environments

OE.Competent_personnel

Personnel using the TOE must have been trained, competent and follow all applicable guidance documentation.

OE. Operational_procedures

Personnel using the TOE must ensure that the HW to be erased is set in such way, that the storage devices of the system can be detected in the correct way.

OE.Reliable_clock

Personnel using the TOE must ensure that the BIOS clock in the system to be erased has correct values.

Security Objectives Rationale

This section provides a rationale for the existence of each assumption and threat. The following table demonstrates that the mapping between the assumptions and threats to the security objectives is complete. The discussion following provides the rationale of coverage for each assumption and threat by IT or non-IT security objectives.

Table 4. Mapping of Threats, Assumptions & Security Objectives

	O.Erasure_process	O.Reporting_content	O.Verificaion_of_erasure	O.Detection_of_storeage_device_capacity	OE.Competent_personnel	OE.Operational_procedures	OE.Reliable_clock
T.Incomplete_overwrite	X			X	X	X	
T.Incorrect_reporting		X	X		X	X	
T.Incorrect_parameter_usage	X		X			X	
A.Competent_users					X		
A.Proper_procedures						X	
A.BIOS_modifications					X	X	
A.System_clock							X

T.Incomplete_overwrite

> *TOE fails to overwrite content of the storage devices or a specified part of the storage devices has not been overwritten, and consumer data can still be found.*

This threat is countered by the TOE security objectives:

- O.Erasure_process
- O.Detection_of_storage_device_capacity

These objectives ensure that the TOE can totally erase (O.Erasure_process) all selected data from a known storage device capacity (O.Detection_of_storage_device_capacity).

The objectives on the environment OE.Competent_personnel and OE.Operational_procedures will support O.Erasure_process since the selection procedures are not totally automatic.

T.Incorrect_reporting

> *TOE fails to report correctly about the result of erasure process and/or the capacity of the storage device.*

This threat is countered by the TOE security objectives:

- O.Reporting_content
- O.Verification_of_erasure

These objectives ensure that the TOE can report (O.Reporting_content) the success of the erasure process (O.Verification_of_erasure).

The objectives on the environment OE.Competent_personnel and OE.Operational_procedures will support O.Reporting_content since the selection procedures (information of selections included to report) are not totally automatic.

T.Incorrect_parameter_usage

> *TOE fails to perform the erasure as set in configuration parameters, which are given to the TOE. With the configuration parameters user can select the following:*
>
> - *Erasure standard*
> - *Storage device(s) and partitions to be erased*

This threat is countered by the TOE security objectives:

- O.Erasure_process
- O.Verification_of_erasure

These objectives ensure that the TOE performs erasure of storage device(s) (O.Erasure_process) as required by user (O.Verification_of_erasure).

The objective on the environment OE.Operational_procedures will support O.Erasure_process since it ensures that the device to be erased is correctly known by the TOE and accepts the given set of parameters.

A.Competent_users

> *The persons using the TOE are trusted, trained, competent and follow the application guidance documentation.*

This assumption is satisfied by the TOE security objective:

- OE.Competent_personnel

This objective ensures that competent and trained personnel operate TOE in a secure manner and they follow all applicable guidance documentation.

A.Proper_procedures

> *The persons using the TOE must have knowledge and proper procedures in order to modify HW to be erased in order to proper detection of storage devices.*

This assumption is satisfied by the TOE security objective:

- OE.Operational_procedures

This objective ensures that HW to be erased by the TOE is set in such way, the storage devices of the system can be detected in the correct way.

A.BIOS_modifications

> *BIOS settings of the HW to be erased must be modified in such way, that they do not prevent the erasure of storage devices.*

This assumption is satisfied by the TOE security objectives:

- OE.Competent_personnel
- OE.Operational_procedures

These objectives ensure that personnel using the TOE are trained and competent (OE.Competent_personnel) to set BIOS of the HW (OE.Operational_procedures) to be erased in such way, that they do not prevent the erasure of storage device(s).

A.System_clock

> *BIOS clock of the HW to be erased must be set to the correct time and date for reporting purposes.*

This assumption is satisfied by the TOE security objective:

- OE.Reliable_clock

This objective ensures that the information of erasure time and date in report are correct (OE.Reliable_clock).

SECURITY REQUIREMENTS

Security Functional Requirements

User Data Protection

FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components

Dependencies: No dependencies

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].

Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Time stamps

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 [not specified] level of audit; and

c) For each audit event type, based on the auditable event definitions of the functional components included in PP/ST, [FDP_RIP.1].

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 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. [Disk/partition identification, number of passes, overwrite pattern, write failures].

Protection of the TSF

FPT_ITI.1 Integrity of exported TSF data

Hierarchical to: No other components

Dependencies: No dependencies

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: MD5 checksum].

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.

Security Assurance Requirements

The assurance level selected for the TOE is EAL3 (methodically tested and checked) augmented with ALC_FLR.3 because it provides appropriate assurance measures for the expected application of the product.

ALC_FLR.3 is an augmentation to the EAL3 requirements. ALC_FLR.3 is included to add assurance for systematic flaw remediation.

Table 5. EAL 3 augmented with ALC_FLR.3 assurance requirements

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 Authorization controls ALC_CMS.3 Implementation representation CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_FLR.3 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

Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Table 6 indicates the requirements that effectively satisfy the individual objectives.

Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target is fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy.

Table 6. Mapping of security objectives and security functional requirements

	FAU_GEN.1: Audit data generation	FDP_RIP.1 Subset residual information protection	FPT_ITI.1: Integrity of exported TSF data
O.Erasure_process		X	
O.Reporting_content	X		
O.Verification_of_erasure			X

O.Detection_of_storage_device_capacity			X

O.Erasure_process

The TOE is capable to erase all addressable data from the storage devices and partitions selected to be erased, in such way that attempting to read original data from the storage will fail.

This TOE security objective is satisfied by the TOE security functional requirements:

- FDP_RIP.1

FDP_RIP.1 specifies that selected information is made unavailable.

O.Reporting_content

The TOE shall provide information of the erasure process, consisting of: erasure success or failure, special area handling, erasure standard and information about areas, which could not be erased.

This TOE security objective is satisfied by the TOE security functional requirement:

- FAU_GEN.1

FAU_GEN.1 specifies that TOE is able to generate an audit record of information mentioned in O.Reporting_content.

O.Verification_of_erasure

The TOE shall perform verification of the erasure process and report the result of the erasure process.

This TOE security objective is satisfied by the TOE security functional requirement:

- FPT_ITI.1

FPT_ITI.1 specifies that report values exported from the TOE are not modified.

O.Detection_of_storage_device_capacity

The TOE shall detect the correct capacity of the storage device in order to perform erasure process in secure way.

This TOE security objective is satisfied by the TOE security functional requirement:

- FPT_ITI.1

FPT_ITI.1 specifies that the TOE sends correct commands in order to detect the correct capacity of storage device.

Requirement Dependency Rational

Dependencies among functional requirement components are satisfied as shown in table below. Brackets are used to express that the dependencies are not satisfied. Reasons are given in the rationale below.

Table 7. Security Functional Requirements dependencies

Security Functional Requirements	Dependencies
FAU_GEN.1: Audit data generation	(FPT_STM.1 : Time Stamps)
FDP_RIP.1 Subset residual information protection	no dependency
FPT_ITI.1: Integrity of exported TSF data	no dependency

FCS_GEN.1 depend on FPT_STM.1 but FPT_STM.1 is not included in this ST because time support is provided by the environment of the TOE (OE.Reliable_clock).

TOE SUMMARY SPECIFICATION

This chapter describes the TOE summary specifications.

TOE Security Functions

This section describes the TOE security functions

SF_Erasure_engine

The TOE erasure process is divided into multiple sequential steps that are executed in order on the entity that is being erased. An erasure process is considered to have finished successfully if every one of its steps has completed without error. The four most commonly encountered erasure steps are the following:

WritePattern: Overwrite all addressable sectors of a volume with a specific byte pattern.

SecureErase: Erase the contents of all addressable sectors and remapped sectors of a volume.

VerifyData: Verify that the volume's addressable contents match with a specific byte pattern.

The **WritePattern** and **SecureErase** steps can terminate if their target volume is physically disconnected or otherwise becomes unavailable. Normal write errors, however, are simply logged and reported, but do not result in the step itself failing.

The verification step, on the other hand, can and will fail if its contents do not match a specified pattern. A failed verification step therefore results in the erasure process being terminated.

SF_Command_and_Control

After an erasure process has been performed, the TOE will perform the verification process in order to determine has the data erasure been successful. User of the TOE has two selections for verification process:

- Full verification; All addressable locations of the storage device(s) will be verified
- Partial verification; The TOE will select the locations from the storage device(s) from where the erasure process will be verified. The size of the verified locations is depended of the size of the storage device.

If verification process detects that erasure has not been performed in correct manner, the TOE will report that erasure process has failed and storage device(s) might not be fully erased from previous data.

All input and output from and to the TOE is protected and cannot be modified without notification by the TOE.

TOE Summary Specification Rationale

This section in conjunction with previous section, the TOE Security Functions, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions

described in the TOE Security Functions are all necessary for the required security functionality in the TSF. Table 8 demonstrates the relationship between security requirements and security functions.

Table 8. Relationship between SFR's and Security Functions

	SF.Erasure_engine	SF.Command_and_control
FDP_RIP.1	X	
FAU_GEN.1		X
FPT_ITI.1		X