RECOVERY LABS®

Security Target for the Secure Data Erasure Software: EraseIT

Authors: Daniel SANZ / Jaime HERENCIA
Date: 24/03/10
Version 1.55eng

Historical versions

VERSION	DATE	AUTHORS	DESCRIPTION
1.0	06/07/09	Daniel SANZ Jaime HERENCIA	First Document
1.1	20/07/09	Daniel SANZ Jaime HERENCIA	Revision 1: - Security assurance requirements (SARs) modification - TOE Description modification adding the physical scope - Inclusion of the SARs and the security requirement rationale
1.2	29/07/09	Daniel SANZ Jaime HERENCIA	Revision 2: - TOE Overview modification - Security Requirements modification - TOE Summary modification
1.3	18/08/09	Daniel SANZ Jaime HERENCIA	Revision 3: - TOE Version
1.4	18/09/09	Daniel SANZ Jaime HERENCIA	Revision 4: - TOE Version - TOE Overview modification - ASSUMPTIONS modification
1.5	30/09/09	Jaime HERENCIA	Revision 5: - ASSUMPTIONS Relationships and Operacional enviroment objectives modifications - TOE Version
1.55	24/03/10	Daniel SANZ Jaime HERENCIA	Revision 6: Product name unification
1.55eng	14/06/10	Jaime HERENCIA Alexis Paez	Revision 7: - Traducción al inglés

Contents Table

ST Introduction

ST reference and TOE reference

The information to identify this document and the TOE is shown below.

ST title:
Security Target for the Secure Data Erasure Software: EraseIT Loop
ST version:
1.55
Date:
2010-03-24
Authors:
Daniel SANZ / Jaime HERENCIA - RECOVERYLABS S.A.
Product:
EraseIT Loop
TOE Identification:
EraseIT Loop V1.73
CC version:
Common Criteria for Information Technology Security Evaluation, Version 3.1 R2
Keywords:
Residual Information Protection, Disk Erasure, Media Security

TOE Overview

Software developed for the secure erasure of data contained in storage devices. Secure erasure process is done by overwriting data. Software runs on a PC-compatible platform and uses I**DE, SATA, SCSI and USB** controllers to access and overwrite the data of the user-selected devices. On USB U3 write-protected partitions the erasure process is NOT executed. **Erasure method is user-configurable**, so it is possible to do the secure erasure following the standards DoD5220.22-M, HMG Infosec Standard No:5, NATO standard, US Navy, NAVSO P-5239-26 – RLL, US Air Force, AFSSI5020, Peter Gutmann patterns, etc. On erasure process completion the **audit information** will be saved in the storage drive from which it can be exported to other storage media.

1.1.1. TOE type

EraseIt Loop is secure erasure software.

EraseIT Loop is an application that can be executed using different bootable resources (CD/DVD, USB, net, etc). It Incorporates its own operating system in order to avoid dependencies and increase compability.

1.1.2. Required non-TOE hardware/software/firmware

EraseIT Loop requirements:

- PC-compatible x86
- 128 Mb RAM
- BIOS configured for booting from external resources.

Sytem specifications:

- Processor: Intel Celeron D 336, 2800 MHz (21 x 133)
- Mother board: ASRock 775i65G
- Mother board chipset: Intel Springdale-G i865G
- RAM: 1024 MB
- BIOS: AMI P.300 (20/03/07)

Controllers:

- SCSI controller: PCS SCSI Adaptec AHA-2940UW
- IDE controller: Intel(R) 82801EB - 24D1
- USB controller: Intel 82801EB ICH5 - USB Controller [A-2/A-3]

Storage devices:

- SCSI storage device: SEAGATE ST39103LW SCSI Disk Device (9 GB, 10000 RPM, Ultra2 SCSI) - LS568113000010161ZJX
- SATA storage device: SEAGATE ST96812AS (60 GB, 5400 RPM, SATA) - 5PJ01493
- USB storage device: SEAGATE ST3802110A USB Device (80 GB, 7200 RPM, Ultra-ATA/100)
- IDE s: SEAGATE ST380215A (80 GB, 7200 RPM, Ultra-ATA/100) - 6QZ6XX52
- Removible USB storage device: USB Flash Memory USB Device (486 MB, USB)

	Scope
Processor: Intel Celeron D 336, 2800 MHz (21 x 133)	×
Mother board: ASRock 775i65G	×
Mother board chipset: Intel Springdale-G i865G	×
RAM: 1024 MB	×
BIOS: AMI P.300 (20/03/07)	×
SCSI controller: PCS SCSI Adaptec AHA-2940UW	×
IDE controller: Intel(R) 82801EB - 24D1	×
USB controller: Intel 82801EB ICH5 - USB Controller [A-2/A-3]	×
SCSI storage device: SEAGATE ST39103LW SCSI Disk Device (9 GB, 10000 RPM, Ultra2 SCSI) -	×

LS568113000010161ZJX	
SATA storage device: SEAGATE ST96812AS (60 GB, 5400 RPM, SATA) - 5PJ01493	×
USB storage device: SEAGATE ST3802110A USB Device (80 GB, 7200 RPM, Ultra-ATA/100)	×
IDE storage device: SEAGATE ST380215A (80 GB, 7200 RPM, Ultra-ATA/100) - 6QZ6XX52	×
Removible USB storage device: USB Flash Memory USB Device (486 MB, USB)	×

✓ In TOE
× Out of TOE

The data in USB U3 write-protected partitions will not be securely erased.

TOE Description

EraseIT Loop is an application for secure data erasure, developed to guarantee the confidentiality of the information stored in IT equipment.

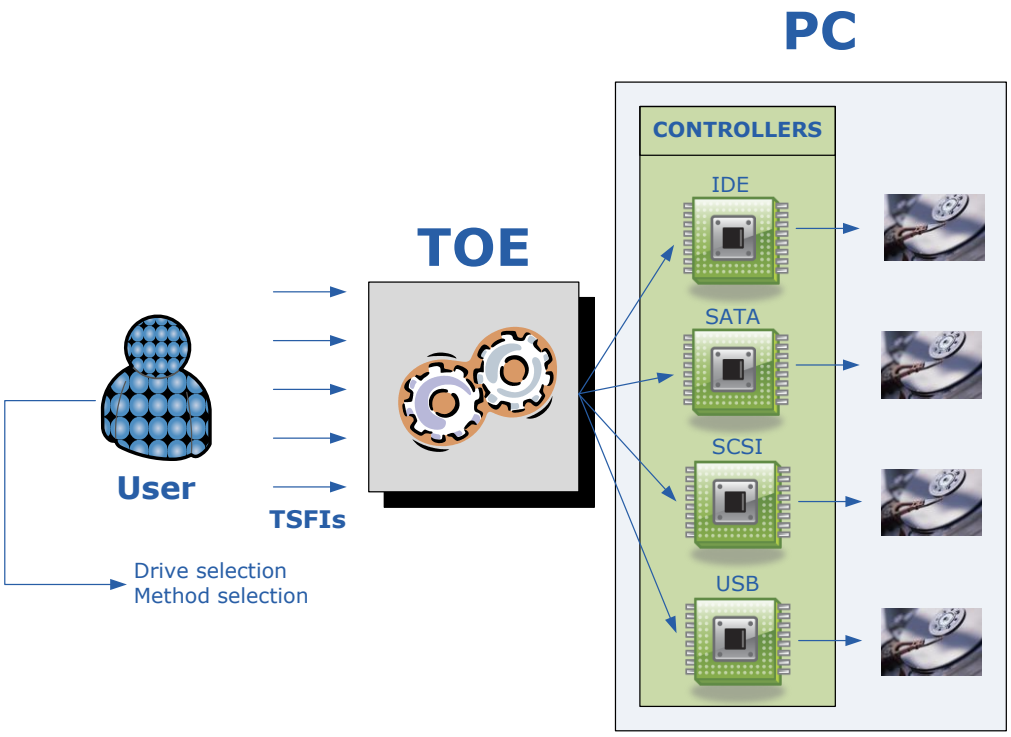
EraseIT Loop allows secure and permanent data deletion from computers that are to be recycled. EraseIT Loop assists you in:

- Avoiding compromising situations:
    - Allowing you to fulfill the measures set out in the Data Protection Act (Spain's LOPD) aimed at preventing access to the information contained in a support or its recovery.
    - **No risk** of confidential information breaches.
    - Without breaking the **digital chain of custody**.
- Simplifies the management of the renovation or removal of IT equipment by optimizing the shipping logistics.

EraseIT Loop offers the user maximum features:

- Performs deletion on all interfaces: IDE, SATA, SCSI, USB, etc.

Configurable to meet international deletion standards: **American DoD 5220-22.M Standard Wipe, HMG Infosec Standard No: 5, NATO Standard, Canadian RCMP TSSIT OPS-II Standard Wipe**, **BSI (German overwrite standard by Federal Office for Information Security)**, etc.



Graph 1

1.1.3. Logical Scope

EraseIT Loop starts by detecting the storage devices connected to the system. The user is able to select the devices that will be securely erased and the erasure method which will be used in the process. Once the configuration is established, the secure erasure process begins and is audited. On process completion, an encrypted report containing the audit information (devices, erasure method and error logs) will be shown. The report also stores a validated erasure date from an external server to guarantee when the process took place.

Functionalities	*Scope*	*Coms.*
Secure data erasure	☑	
Device selection	☑	
Erasure method selection (DoD5220.22-M, HMG Infosec Standard No:5,…)	☑	
Audit	☑	
Encrypted report	✓	
External server NIST date validation	✓	
License handler	✓	
Web control panel	×	Add-on

☑ Affects security functionality
✓ In TOE
× Out of TOE

1.1.4. Physical scope

EraseIT Loop is a software application so hardware/firmware is excluded from the external components point of view (see Graph 1).

Conformance claims

TOE is in accordance with:

- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 R2
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 3.1 R2
- EAL 1 + ALC_FLR.1 + ASE_SPD.1 + ASE_OBJ.2 + ASE_REQ.2

Terminology

secure erasure process	Storage device overwriting process which guarantees the confidentiality of the information stored in it.
storage device	Mass storage devices. Ej. HDD, USB storage device, etc.
secure erasure process operation	Secure erasure process in all the sectors of a storage device.
secure erasure method	Secure erasure operation compound.
the user	Any user who runs the application.
secure erasure method selection functions	Compound of functions which helps the user in the secure erasure method selection.
storage devices selection functions	Compound of functions which helps the user in the device selection.

2.Security problem definition

Introduction

The security problem is the confidentiality of the information stored in storage devices.

Threats

Name	*Description*
T.DATA_RECOVERY	Once the secure erasure process has finished, a user with access to the storage device can recover the original data stored.

Organisational security policies

Name	*Description*
P.AUDIT	The application will provide an audit facility that will allow the analysis of operations on large bases of IT equipment.
P.METHOD_SELECTION	The application will allow the user to select the secure erasure method, in order to execute the process according to the desired standard. (Ex. DoD5220.22-M, HMG Infosec Standard No:5, …).
P.DEVICE_SELECTION	The application will allow the user to select the storage devices in which the secure erasure process will be executed.

Assumptions

Name	*Description*
A.CODE	Its assumed that no code will be executed by an attacker before TOE boots.

Security objectives

Security objectives for the TOE

Name	*Description*
O.DATA_ERASURE	The application will erase the information stored in the storage devices in which the secure erasure process is executed.
O.AUDIT	The application will generate a log with the secure erasure process information.
O.METHOD_SELECTION	The application will allow the user to select the secure erasure method.
O.DEVICE_SELECTION	The application will allow the user to select the storage devices in which the secure erasure process will be executed.

Security objectives for the operational environment

Name	*Description*
OE.CODE	The operational enviroment should guarantee that no code can be executed before TOE boots.

Relation between security objectives and the security problem definition

2.1.1. Tracing between security objectives and the security problem definition

OBJECTIVES	***THREATS***	***POLICIES***			***ASSUMPTIONS***
	T.DATA_ RECOVERY	*P.AUDIT*	*P.METHOD_ SELECTION*	*P.DEVICE_ SELECTION*	*A.CODE*
O.DATA_ ERASURE	☑				
O.AUDIT		☑			
O.METHOD_ SELECTION			☑		
O.DEVICE_ SELECTION				☑	
OE.CODE					☑

2.1.2. Providing a justification for the tracing

O.DATA_ERASURE – T.DATA_RECOVERY

If the threat that a user could recover the data stored on a device can be averted, the confidentiality of this data will be guaranteed.

O.AUDIT – P.AUDIT

If a log with the secure erasure process information is generated with a proper policy, the audit objective will be achieved.

P.METHOD_SELECTION – P.METHOD_SELECTION

If a proper security policy is applicated, the user will be able to select a secure erasure method.

P.DEVICE_SELECTION - P.DEVICE_SELECTION

If a proper security policy is applicated, the user will be able to select the storage devices to be be securely erased.

A.CODE- OE.CODE

It it assumed that no code could be executed before TOE boots, the objective of guarantee that no code will be executed before TOE boots will be achieved.

Security objectives: conclusion

If preventing the threats and implementing the security policies is achieved, the secure problem will be resolved.

Extended Components Definition

It is not necessary an extended component definition.

Security requirements

Security functional requirements

Class FDP		
FDP_RIP.1 Residual information protection		
	FDP_RIP.1	The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: deallocation of the resource from] the following objects: [assignment: storage devices].
Class FAU		

FAU_GEN.1 Security audit data generation		
	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: each secure erasure process operation].
	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, 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: secure erasure method used, storage device]. NOTA: the secure erasure method and the storage devices to be secure erased have been selected by the user. See FMT_SMF.1
	Se elimina la dependencia de *FMT_STM.1 – Time stamps* debido a que el TOE no proporciona una fuente de tiempo, se utiliza una fuente externa al TOE.	
Class FMT		
FMT_SMF.1 - Specification of Management Functions		
	FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [assignment: select the secure erasure method, select the storage devices to be secure erased].

Relation between SFRs and security objectives

Security Objectives	SFRs		
	FDP_RIP.1	FAU_GEN.1	FMT_SMF.1
O.DATA_ ERASURE	☑		
O.AUDIT		☑	
O.METHOD_ SELECTION			☑
O.DEVICE_ SELECTION			☑

Tracing between SFRs and the security objectives for the TOE

O.DATA_ERASURE – FDP_RIP.1

If TSF guarantees that the information stored in a storage device is securely erased, the objective of guaranteeing data confidentiality will be achieved.

O.AUDIT – FAU_GEN.1

If TSF registers the information of the secure erasure process events, the audit objective will be achieved.

O.METHOD_SELECTION – FMT_SMF.1

If TSF allows the user, there is only one role, to execute functions of selecting secure erasure method, the objective of allowing the user to select the secure erasure method following different standards (Ex. DoD5220.22-M, HMG Infosec Standard No:5, etc.) will be achieved.

O.DEVICE_SELECTION - FMT_SMF.1

If TSF allows the user, there is only one role, to execute the functions of selecting the storage devices to be secure erased, the objective of allowing the user to select the storage devices to be secure erased will be achieved.

Security assurance requirements (SARs)

Class ADV: Development		
ADV_FSP.1 Basic functional specification		
	ADV_FSP.1.1D	The developer shall provide a functional specification.
	ADV_FSP.1.2D	The developer shall provide a tracing from the functional specification to the SFRs.
	ADV_FSP.1.1C	The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.
	ADV_FSP.1.2C	The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.
	ADV_FSP.1.3C	The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.
	ADV_FSP.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	ADV_FSP.1.2E	The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.
Class AGD: Guidance documents		
AGD_OPE.1 Operational user guidance		
	AGD_OPE.1.1D	The developer shall provide operational user guidance.
	AGD_OPE.1.1C	The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

	AGD_OPE.1.2C	The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
	AGD_OPE.1.3C	The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
	AGD_OPE.1.4C	The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
	AGD_OPE.1.5C	The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
	AGD_OPE.1.6C	The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.
	AGD_OPE.1.7C	The operational user guidance shall be clear and reasonable.
	AGD_OPE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1 Preparative procedures		
	AGD_PRE.1.1D	The developer shall provide the TOE including its preparative procedures.
	AGD_PRE.1.1C	The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE

		in accordance with the developer's delivery procedures.
	AGD_PRE.1.2C	The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
	AGD_PRE.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	AGD_PRE.1.2E	The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.
ALC_CMC.1 Labeling of the TOE		
	ALC_CMC.1.1D	The developer shall provide the TOE and a reference for the TOE.
	ALC_CMC.1.1C	The TOE shall be labeled with its unique reference.
	ALC_CMC.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ALC_CMS.1 TOE CM coverage		
	ALC_CMS.1.1D	The developer shall provide a configuration list for the TOE.
	ALC_CMS.1.1C	The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs
	ALC_CMS.1.2C	The configuration list shall uniquely identify the configuration items.
	ALC_CMS.1.1E	The evaluator shall confirm that the information provided meets all

		requirements for content and presentation of evidence.
ALC_FLR.1 Basic flaw remediation		
	ALC_FLR.1.1D	The developer shall document flaw remediation procedures addressed to TOE developers.
	ALC_FLR.1.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
	ALC_FLR.1.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
	ALC_FLR.1.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
	ALC_FLR.1.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.
	ALC_FLR.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
Class ASE: Security Target evaluation		
ASE_CCL.1 Conformance claims		
	ASE_CCL.1.1D	The developer shall provide a conformance claim.
	ASE_CCL.1.2D	The developer shall provide a conformance claim rationale.
	ASE_CCL.1.1C	The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance

	ASE_CCL.1.2C	The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.
	ASE_CCL.1.3C	The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.
	ASE_CCL.1.4C	The CC conformance claim shall be consistent with the extended components definition.
	ASE_CCL.1.5C	The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
	ASE_CCL.1.6C	The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
	ASE_CCL.1.7C	The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
	ASE_CCL.1.8C	The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
	ASE_CCL.1.9C	The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
	ASE_CCL.1.10C	The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

	ASE_CCL.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_ECD.1 Extended components definition		
	ASE_ECD.1.1D	The developer shall provide a statement of security requirements.
	ASE_ECD.1.2D	The developer shall provide an extended components definition.
	ASE_ECD.1.1C	The statement of security requirements shall identify all extended security requirements.
	ASE_ECD.1.2C	The extended components definition shall define an extended component for each extended security requirement.
	ASE_ECD.1.3C	The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.
	ASE_ECD.1.4C	The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.
	ASE_ECD.1.2C5	The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.
	ASE_ECD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	ASE_ECD.1.2E	The evaluator shall confirm that no extended component can be clearly expressed using existing components.
ASE_INT.1 ST introduction		
	ASE_INT.1.1D	The developer shall provide an ST introduction.

	ASE_INT.1.1C	The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.
	ASE_INT.1.2C	The ST reference shall uniquely identify the ST.
	ASE_INT.1.3C	The TOE reference shall identify the TOE
	ASE_INT.1.4C	The TOE overview shall summarize the usage and major security features of the TOE.
	ASE_INT.1.5C	The TOE overview shall identify the TOE type.
	ASE_INT.1.6C	The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.
	ASE_INT.1.7C	The TOE description shall describe the physical scope of the TOE.
	ASE_INT.1.8C	The TOE description shall describe the logical scope of the TOE.
	ASE_INT.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	ASE_INT.1.2E	The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.
ASE_OBJ.2 Security objectives		
	ASE_OBJ.2.2D	The developer shall provide a statement of security objectives.
	ASE_OBJ.2.1D	The developer shall provide a security objectives rationale.
	ASE_OBJ.2.1C	The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

	ASE_OBJ.2.2C	The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
	ASE_OBJ.2.3C	The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.
	ASE_OBJ.2.4C	The security objectives rationale shall demonstrate that the security objectives counter all threats.
	ASE_OBJ.2.5C	The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.
	ASE_OBJ.2.6C	The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.
	ASE_OBJ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_REQ.2 Derived security requirements		
	ASE_REQ.2.1D	The developer shall provide a statement of security requirements.
	ASE_REQ.2.2D	The developer shall provide a security requirements rationale.
	ASE_REQ.2.1C	The statement of security requirements shall describe the SFRs and the SARs.
	ASE_REQ.2.2C	All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.
	ASE_REQ.2.3C	The statement of security requirements shall identify all operations on the

		security requirements.
	ASE_REQ.2.4C	All operations shall be performed correctly.
	ASE_REQ.2.5C	Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.
	ASE_REQ.2.6C	The security requirements rationale shall trace each SFR back to the security objectives for the TOE.
	ASE_REQ.2.7C	The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.
	ASE_REQ.2.8C	The security requirements rationale shall explain why the SARs were chosen.
	ASE_REQ.2.9C	The statement of security requirements shall be internally consistent.
	ASE_REQ.2.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ASE_TSS.1 TOE summary specification		
	ASE_TSS.1.1D	The developer shall provide a TOE summary specification.
	ASE_TSS.1.1C	The TOE summary specification shall describe how the TOE meets each SFR.
	ASE_TSS.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	ASE_TSS.1.2E	The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.
ASE_SPD.1 Security problem definition		

	ASE_SPD.1.1D	The developer shall provide a security problem definition.
	ASE_SPD.1.1C	The security problem definition shall describe the threats.
	ASE_SPD.1.2C	All threats shall be described in terms of a threat agent, an asset, and an adverse action.
	ASE_SPD.1.3C	The security problem definition shall describe the OSPs.
	ASE_SPD.1.4C	The security problem definition shall describe the assumptions about the operational environment of the TOE.
	ASE_SPD.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
Class ATE: Tests		
ATE_IND.1 Independent testing – conformance		
	ATE_IND.1.1D	The developer shall provide the TOE for testing.
	ATE_IND.1.1C	The TOE shall be suitable for testing.
	ATE_IND.1.1E	The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
	ATE_IND.1.2E	The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.
Class AVA: Vulnerability assessment A		
AVA_VAN.1 Vulnerability survey		
	AVA_VAN.1.1D	The developer shall provide the TOE for testing.
	AVA_VAN.1.1C	The TOE shall be suitable for testing.
	AVA_VAN.1.1E	The evaluator shall confirm that the information provided meets all

		requirements for content and presentation of evidence.
	AVA_VAN.1.2E	The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.
	AVA_VAN.1.3E	The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

SARs and the security requirement rationale

The specified SARS have been chosen based on market demand.

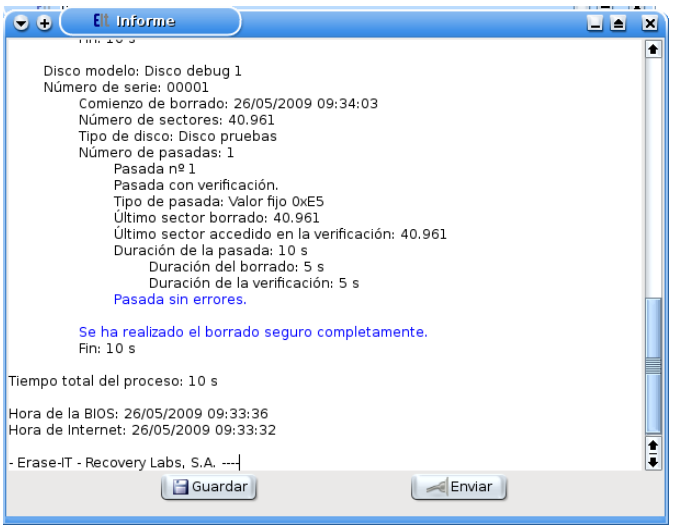
TOE summary specification

SF.OVERWRITE

TSF deals with the secure erasure of the storage devices by overwriting the data stored. The erasure method is composed of random and fixed overwriting passes.

SF.AUDIT

TSF generates a secure erasure report that stores information relative to the secure erasure process. It stores the start and end of the operations, the storage devices technical information and the secure erasure method used in the execution.



SF.METHOD_SELECTION

TSF allows the user to select the secure erasure method to execute in the secure erasure process. The secure erasure method is composed of at least a fixed/random overwriting pass. It is posible to run the pass with verification.

TSF allows the user to do this in two different ways:

- Predefined method
  TSF allows the user to select the secure erasure method from a list of standards (DoD5220.22-M, NATO standard, US Navy, NAVSO P-5239-26 – RLL, US Air Force, AFSSI5020, Peter Gutmann patterns, etc.)

- User defined
  TSF allows the user to customize the secure erasure method in order to support other standards (Ej. HMG Infosec Standard No:5).

SF.DEVICE_SELECTION

TSF allows the user to select the storage devices to be securely erased.

SF.OVERWRITE assures that the data stored in the storage devices has been securely erased. So FDP_RIP.1 is fullfilled.

SF.AUDIT assures the audit of the secure erasure process with the storage devices and secure erasure methods, and the start and end of all the processes. So FAU_GEN.1 is fullfilled.

SF.METHOD_SELECTION and SF.DEVICE_SELECTION assures that the user is able to select the storage devices to be securely erased and the secure erasure method. So FMT_SMF.1 is fullfilled.

SFRs	Security functionalities			
	SF.OVERWRITE	SF.AUDIT	SF.METHOD_ SELECTION	SF.DEVICE_ SELECTION
FDP_RIP.1	☑			
FAU_GEN.1		☑		
FMT_SMF.1			☑	☑