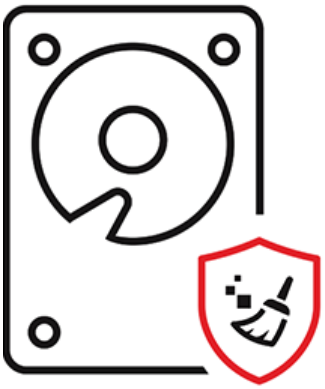

BitRaser Drive Eraser

Version 3.0.0.6 (TOE)

Security Target

Document Version 1.1

REVISION HISTORY

Version	Date	Revision	Author
1.0	11th Jan 2021	First Issue	Amit Shukla
1.1	13th Jan 2023	Updated: Drive types, List of Erasure Methods, Kernel version	Amit Shukla

ACRONYMS

AES	**ADVANCED ENCRYPTION STANDARD**
ATA	**ADVANCED TECHNOLOGY ATTACHMENT**
BIOS	**BASIC INPUT-OUTPUT SYSTEM**
CC	**COMMON CRITERIA**
EAL	**EVALUATION ASSURANCE LEVEL**
GUI	**GRAPHICAL USER INTERFACE**
HPA/DCO	**HOST PROTECTED AREA/DEVICE CONFIGURATION OVERLAY**
HTTPS	**HYPERTEXT TRANSFER PROTOCOL SECURE**
IDE	**INTEGRATED DEVELOPMENT ENVIRONMENT**
NA	**NOT APPLICABLE**
NVME	**NON-VOLATILE MEMORY EXPRESS**
PC	**PERSONAL COMPUTER**
PDF	**PORTABLE DOCUMENT FORMAT**
RAID	**REDUNDANT ARRAY OF INEXPENSIVE DISKS**
RAM	**RANDOM-ACCESS MEMORY**
SAS	**SERIAL ATTACHED SCSI**
SATA	**SERIAL ADVANCED TECHNOLOGY ATTACHMENT**
SD CARD	**SECURE DIGITAL CARD**
SFP	**SECURITY FUNCTION POLICY**
SFR	**SECURITY FUNCTIONAL REQUIREMENTS**
SSD	**SOLID STATE DRIVE**
ST	**SECURITY TARGET**
SVGA	**SUPER VIDEO GRAPHICS ARRAY**
TOE	**TARGET OF EVALUATION**
TSF	**TOE SECURITY FUNCTION**
USB	**UNIVERSAL SERIAL BUS**

Contents

1. SECURITY TARGET INTRODUCTION

This section covers the identification of the **Security Target** (ST) and **Target of Evaluation** (TOE). The TOE is **BitRaser Drive Eraser** developed by **Stellar Information Technology**. The TOE is being evaluated as a drive erasure software application.

The Security Target contains the following additional sections:

- Conformance Claims (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- Extended Components Definition (Section 5)
- Security Requirements (Section 6)
- TOE Summary Specification (Section 7)

1.1. Security Target Reference

ST Title – BitRaser Drive Eraser Version 3.0.0.6 Security Target

ST Version – Version 1.1

ST Date – January 13th, 2023

1.2. TOE Reference

The TOE is the "BitRaser Drive Eraser" software which is contained in a bootable ISO.

TOE/ISO	File Name	Version	MD5 Hash
TOE -BitRaser Drive Eraser	BITRASER	3.0.0.6	4468c1fc78241d0641001a72a68afd65
Bootable ISO	Bitraser-x86_64.iso	6.1.4	15702a531d910413c21458da041d8b99

TOE Developer – Stellar Information Technology Private Limited

TOE with the USB lock key has been considered for the purpose of evaluation. This means that the licenses of the TOE have been stored in the USB lock key.

1.3. TOE Overview

The Target of Evaluation (TOE) is **BitRaser Drive Eraser**. The TOE is a portable software providing permanent data erasure of storage devices. This software erases storage devices

including all its partitions, to prevent the recovery of sensitive data that is no longer required by its user.

The TOE is delivered inside an ISO file. The ISO file is a Linux-based bootable image, using which a bootable media is created. The bootable media is used for booting a PC to a state where the TOE runs in RAM and the storage drives attached to the Host PC can be securely erased. The TOE can erase Magnetic Media: PATA, SATA, SAS hard drives, Flash based media: SSD, NVMe, Flash based USB drives (Pen Drives, Thumb Drives, Flash Memory Drives, Memory Sticks), and memory cards following the erasure algorithm selected by the user before initiating the storage media erasure. The TOE erases the media based on the type of media identified by it except for USB interface. For any media connected over USB interface, it is treated as USB device. TOE also supports reading and writing ATA commands for detection and removal of HPA/DCO along with the erasure of remapped sectors (remapped sectors are the bad sectors that have been replaced by spare sectors of the hard drive). The users can graphically see the progress of erasure through TOE's user interface.

The user of the TOE can erase the storage media in accordance with the selected erasure algorithm from the GUI of the TOE. The outcome of the erasure process, success, or failure, is communicated to the user through the user interface of the TOE. Also, the audit log data collected from the erasure event is stored in the form of a report.

The license source of the TOE stores the licenses used for verifying, whether a user has a right to access an operation.

Note:

Based on the license source, three variants of the **BitRaser Drive Eraser** are available**.**

The variant of **BitRaser Drive Eraser** that is used in association with a USB Lock Key that holds the license, **was evaluated**.

There are other non-evaluated variants of the **BitRaser Drive Eraser** which are designed to work along with **BitRaser Admin Console or BitRaser Cloud Server**. The different license sources of **BitRaser Drive Eraser** are summarized below:

License Source	Characteristics

BitRaser Cloud Server	**BitRaser Drive Eraser** is used in association with **BitRaser Cloud Server** that holds the licenses. However, this variant of the "BitRaser Drive Eraser" software was excluded from evaluation.
BitRaser Admin Console	**BitRaser Drive Eraser** is used in association with **BitRaser Admin Console** that holds the licenses. However, this variant of the "BitRaser Drive Eraser" software was excluded from evaluation.
USB Lock Key	**BitRaser Drive Eraser** is used in association with a **USB Lock Key** that holds the licenses. This variant of the "BitRaser Drive Eraser" is the Target of Evaluation **(TOE).**

TOE Features

S. No.	Feature	Status
1	Drive Erasure with Total Verification i. US Department of Defense, DoD 5220.22-M (3 Passes) ii. NIST 800-88 Clear (1 or 3 Passes) **For Magnetic Media: PATA, SATA, SAS, Flash based Media: SSD, NVMe** - 1 Pass **For Removable USB Drives, Memory Cards** - 3 Passes iii. NIST 800-88 Purge **For Magnetic Media: PATA, SATA, SAS, Flash based Media: SSD, NVMe** – sanitization is done as per NIST standard. **For Flash based Media: Removable USB Drives,** the sanitization method NIST Clear 3 Pass is executed as per NIST recommendation. **For Flash based Media: Memory Cards,** as Purge is not applicable, NIST Clear - 3 Pass is executed. iv. BitRaser Secure & SSD Erasure **For Magnetic Media: PATA, SATA, SAS, Flash based Media: SSD, NVMe** – sanitization is done as per NIST standard. **For Flash based Media: Removable USB Drives,** the sanitization method NIST Clear 3 Pass is executed as per NIST recommendation.	**Evaluated**

	For Flash based Media: Memory Cards, as Purge is not applicable, NIST Clear - 3 Pass is executed. v. British HMG IS5 Enhanced Standard (3 Passes) **For Magnetic Media: PATA, SATA, SAS**: DoD 5220.22-M (3 Passes) is executed as per the standard. **Flash based Media: SSD, NVMe**: DoD 5220.22-M (3 Passes) is executed and ATA Security feature set's SECURITY ERASE UNIT command is executed, if supported. **For Removable USB Drives, Memory Cards**: DoD 5220.22-M (3 Passes) is executed as per the standard. (Refer table in section 1.4.2 for the complete list of erasure algorithms, including those not under evaluation)	
2	Remapped Sectors Erasure **For Magnetic Media: PATA, SATA, SAS** if remapped sectors are available **Flash based Media: SSD** if remapped sectors are available	**Evaluated**
3	HPA/DCO Removal **For Magnetic Media: PATA, SATA, SAS** if HPA/DCO is available **Flash based Media: SSD** if HPA/DCO is available	**Evaluated**
4	Fingerprint Signature After Erasure	**Evaluated**
5	Erasure of PATA, SATA, SAS, SSD, NVMe, USB drives, and memory cards	**Evaluated**
6	Erasure of block sizes other than 512 bytes	**Evaluated**
7	Hex Viewer	**Evaluated**
8	Export Report	**Not Evaluated**
9	RAID Dismantling	**Not Evaluated**
10	Support for Different Keyboard Layouts	**Not Evaluated**
11	Bad Sector Limit to Abort Erasure	**Not Evaluated**
12	Disk Initialization After Erasure	**Not Evaluated**

For the purpose of evaluation, BitRaser Drive Eraser with the USB lock key has been considered. This means that the licenses of the TOE have been stored in the USB lock key.

1.3.1. TOE Security Features

LEGITIMATE_USE: The TOE ensures that it is only used legitimately.

COMPLETE_ERASURE: The TOE ensures that upon successful completion of the erasure, the drive is fully erased in accordance with the selected erasure standard. The indicator of the completeness of the erasure can be relied upon and in any case of incomplete erasure, the indicator shall not indicate successful erasure.

1.3.2. TOE Type

The TOE Type is a drive erasure software executing on a Host PC.

1.3.3. Non-TOE Hardware/Software/Firmware required by the TOE

The TOE requires the following non-TOE hardware/software/firmware:

1.3.3.1. Hardware

The TOE must run on the hardware that meets or exceeds the requirements listed in this section. The hardware must also have the physical connections that work with the media that have to be erased.

- Processor - x86 or x64
- RAM – 1 GB Minimum, 2 GB Recommended
- USB Port and/or an optical media drive with an option in the BIOS to boot computer from USB device or optical media.
- Other – SVGA or higher video support with minimum resolution supported: 1024*768
- USB lock key containing the licenses is required to be connected to the system on which the TOE is being run. This lock is supplied to the user, as mentioned in the section “1.5. Deliverables to End Users” of this document.

1.3.3.2. Software

TOE is software that runs on Linux based operating system (Arch Linux with kernel version 6.1.4).

1.3.3.3. Firmware

TOE assumes that storage devices are loaded with a functional system firmware. Also, the BIOS firmware of the computer must be functioning correctly to run the TOE.

1.3.3.4 TOE and Non TOE Components

The following table identifies different components and indicates whether or not each component is in the TOE:

TOE or Environment	Component	Description
TOE	Executable Binary	The TOE is the executable software inside the bootable ISO image.
Environment **(Not Evaluated)**	System Requirements	Processor - x86 or x64 RAM – 1 GB Minimum, 2 GB Recommended USB Port or an optical media drive with an option in the BIOS to boot computer from USB device or optical media. Functional firmware of BIOS and storage device. Other – SVGA or higher video support, the minimum resolution supported: 1024*768
Environment **(Not Evaluated)**	Linux based Operating System	Arch Linux with kernel version 6.1.4 - delivered as an ISO image for booting a PC to a state where the TOE is running in RAM
Environment **(Not Evaluated)**	Target Devices	PATA, SATA, SAS hard drives, SSD, NVMe, USB drives, and memory cards identified as a candidate for erasure.
Environment **(Not Evaluated)**	Audit Data Storage	The location where the audit data is stored and is located separately from the TOE. The data can be stored on any form of file storage medium.
Environment **(Not Evaluated)**	USB Lock Key	Lock key with USB interface that carries the erasure licenses of the TOE.

1.4. TOE Description

1.4.1. Physical Scope of the TOE

The physical scope of the TOE consists of the TOE software. The licenses are not part of the TOE but are used for controlling access to the TOE functions. The software constituting the TOE is an executable software that is executed from the RAM of the Host PC.
Once the ISO file is stored on a bootable media and a Host PC is booted from that media, the executable software of the TOE runs from the RAM of the Host PC.

1.4.2. Logical Scope of the TOE

The logical scope of the TOE includes the following security functions:

Legitimate Use: The TOE implements measures to make sure that the TOE is used by the authorized user only. The authorization to use the TOE is decided on the basis of availability of the user licenses, as obtained from the USB lock key.

Complete Erasure: The TOE implements a set of erasure functions that are suitable for the drives connected to the Host PC. These are:

1. Using the firmware primitives of each disk, the TOE implements the erasure protocol logic and ensures secure erasure of the drive in full conformance with the applicable standards. To ensure complete erasure, the TOE verifies the erasure results after each step and before completing the erasure.
2. The TOE also implements several erasure algorithms but not all of them are included in the logical scope. Also, for all media types (i.e. PATA/ SATA/ SAS/ SSD/ NVMe/ USB/ Memory Cards) the implemented erasure algorithms in TOE can be used to erase block sizes other than 512 bytes (if available) and for certain media types (like Magnetic Media: PATA, SATA, SAS and Flash based Media: SSD), if remapped sectors or HPA/DCO are available in them, the implemented erasure algorithms in TOE can be used to erase those remapped sectors or HPA/DCO. The following table provides the complete list of the algorithms that the TOE can implement and the algorithms included in the logical scope are denoted with a 'YES' in the 'Included in Evaluation Scope' column:

Erasure Algorithm	Passes	Included in Evaluation Scope
US Department of Defense, DoD 5220.22-M	3	**Yes**
NIST 800-88 Clear **For Magnetic Media: PATA, SATA, SAS, Flash based Media: SSD, NVMe** - 1 Pass **For Removable USB Drives, Memory Cards** - 3 Passes	1 or 3	**Yes**
NIST 800-88 Purge **For Magnetic Media: PATA, SATA, SAS, Flash based Media: SSD, NVMe** – sanitization is done as per NIST standard. **For Flash based Media: Removable USB Drives,** the sanitization method NIST Clear 3 Pass is executed as per NIST recommendation. **For Flash based Media: Memory Cards,** as Purge is not applicable, NIST Clear - 3 Pass is executed.	NA	**Yes**
British HMG IS5 Enhanced Standard **For Magnetic Media: PATA, SATA, SAS**: US Department of Defense, DoD 5220.22-M (3 Passes) is executed as per the standard. **Flash based Media: SSD, NVMe**: US Department of Defense, DoD 5220.22-M (3 Passes) is executed and ATA Security feature set's SECURITY ERASE UNIT command is executed, if supported. **For Removable USB Drives, Memory Cards**: US Department of Defense, DoD 5220.22-M (3 Passes) is executed as per the standard.	3	**Yes**
BitRaser Secure & SSD Erasure **For Magnetic Media: PATA, SATA, SAS, Flash based Media: SSD, NVMe** – sanitization is done as per NIST standard.	NA	**Yes**

For Flash based Media: Removable USB Drives, the sanitization method NIST Clear 3 Pass is executed as per NIST recommendation. **For Flash based Media: Memory Cards,** as Purge is not applicable, NIST Clear - 3 Pass is executed.		
US Department of Defense, DoD 5220.22-M (ECE)	7	**No**
US Department of Defense, DoD 5200.28-STD	7	**No**
Russian Standard - GOST-R-50739-95	2	**No**
B. Schneier's algorithm	7	**No**
German Standard, VSITR	7	**No**
US Army AR 380-19	3	**No**
North Atlantic Treaty Organization-NATO Standard	7	**No**
US Air Force, AFSSI 5020	3	**No**
Canadian CSEC ITSG-06 (1-3 Passes)	1-3	**No**
NSA 130-1	3	**No**
British HMG IS5 Baseline Standard	1	**No**
NAVSO P-5239-26	3	**No**
NCSC-TG-025	3	**No**
Peter Gutmann	35	**No**
Pfitzner algorithm	33	**No**
Zeroes	1	**No**
Pseudo-random	1	**No**
Pseudo-random & Zeroes	2	**No**
Random Random Zero	6	**No**

1.5. Deliverables to End Users

The guidance documentation specified for the usage of the product is delivered to the customers, in a softcopy, together with the product and the USB lock key. The product box contains the USB lock key containing the licenses and a bootable USB drive (the bootable

ISO of the TOE is written on this USB drive). The guidance documentation contains all the information for installation, initialization, configuration, and usage of the TOE in accordance with the requirements of the Security Target.

Guidance Documentation Title: BitRaser Drive Eraser – User Guide ver 3.0

2. CONFORMANCE CLAIMS

2.1. CC Version

The ST and TOE claim conformance to Common Criteria v3.1 Revision 5 Part 1, Common Criteria v3.1, Revision 5 Part 2, and Common Criteria v3.1 Revision 5 Part 3.

The ST claims conformance to the following Protection Profiles and Packages: **None.**

The ST claims package conformance to the following: **Evaluation Assurance Level EAL2.**

2.2. Conformance Claims Rationale

The ST does not claim conformance to any Protection Profile. Therefore, the Conformance Claims Rationale is not applicable.

3. SECURITY PROBLEM DEFINITION

This section describes the security threats for the TOE, organizational security policies, and specific conditions that are assumed related to the TOE and its environment. Each security problem definition is given an identifier consisting of a prefix and a short name. Threats for the TOE are identified by prefix **T,** Organizational Security Policies are identified by prefix **OP** and the assumptions for the environment are identified by prefix **A**.

3.1. Threats

There are threats to TOE itself and therefore TOE is also responsible for addressing these threats in the environment in which it is being operated. The expertise of the attacker for all the threats is assumed at a moderately sophisticated level. The following are threats addressed by the TOE:

T.INCOMPLETE_ERASURE

An attacker succeeds in manipulating the erasure data of the TOE through a legitimate interface in a manner that reports the incomplete erasure of a drive as complete in a manner not detected by the user of the TOE.

T.UNAUTH_USER

An unauthorized user obtains the physical medium which contains the TOE and uses it to perform erasure operation on a storage device for which there has been no authorization.

3.2. Organizational Security Policies

The TOE addresses the following organizational security policies:

OP.ERASE

The TOE will provide measures for erasing data contained on storage devices on a target system as well as sufficient assurance that the data contained on the storage devices was erased, and that the erasure method was sufficient for permanent erasure. The TOE must erase the data in conformance with the standards of the erasure method selected by the user.

The organization utilizing the TOE has defined and enforced a media erasing policy that covers the minimum:

1. The timing when erasing must occur
2. Allowed erasure methods
3. Handling the erasing of all volatile, non-volatile, and EPROM/EEPROM memories
4. Handling of erasure of classified data and the classifications before and after erasure
5. Erasure of media when using encryption and decryption software.
6. User of the TOE must be able to erase media only with the erasure algorithms sufficient to meet the security requirements of the organization using the TOE.

OP.RAID

The TOE is capable of securely erasing RAID disks. However, if the RAID disks remain switched on after the completion of the erasure, the RAID control software may restore some of the information of the disks from associated remote disks. The organization using the TOE must ensure that its policies for handling the erasure of RAID disks take this possibility into account and, if deemed unacceptable, define the measures required for removing the eventuality.

OP.PDF

The erasure reports generated by the TOE are tagged with a digital identifier for authenticity. The report is stored on a USB drive in a PDF format. The organization using the TOE must perform a risk assessment and determine whether saving the reports in PDF is acceptable by the organization's policies and ensure that the users of the TOE are aware of this policy.

OP.CLEAN

An organization using the TOE has defined a security policy for the host in which the TOE is used. This policy must define the minimum security countermeasures required to be in place to reduce the probability of malicious software in the localhost, or the firmware of the drive to be erased, which may prevent the TOE from successfully erasing the drive intended.

3.3. Assumptions

The specific conditions listed in this section are assumed to exist in the environment wherein the TOE is used. These assumptions are necessary as a result of practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

A.PLATFORM

The TOE is assumed to be running from the RAM of the host computer that has been booted using the Bootable USB drive/Optical Media for erasing connected storage devices on the host computer. This includes the underlying platform and the runtime environment it provides to the TOE.

A.PROPER_USE

The user of the TOE is not willfully negligent or hostile and uses the software in compliance with the applied enterprise security policy.

4. SECURITY OBJECTIVES

This section describes the security objectives for the TOE and the security objectives for the environment of the TOE. Each security objective is given an identifier consisting of a prefix and a short name. Security objectives for the TOE are identified by prefix **O** and the security objectives for the environment are identified by prefix **OE**.

4.1. Security Objectives for the TOE

The following are the security objectives for the TOE:

O.COMPLETE_ERASURE

The TOE ensures that upon successful completion of the erasure, the drive is fully erased, in accordance with the selected erasure algorithm defined under the media erasing policy of the organization (OP.ERASE). The completeness of the erasure indicated by the TOE can be relied upon and in any case of incomplete erasure (T.INCOMPLETE_ERASURE), the indicator shall not indicate a successful erasure.

O.LEGIT_USE

The TOE ensures that it is only used in legitimate manners (A.PROPER_USE). The TOE also ensures that it can't be used by any unauthorized user (T.UNAUTH_USER).

4.2. Security Objectives for the Operational Environment of the TOE

The following security objectives apply to the operational environment of the TOE:

OE.PLATFORM

The TOE is to be running from the RAM of the host computer that has been booted using the Bootable USB drive/Optical Media for erasing connected storage devices on the host computer (A.PLATFORM). As a caveat, this may require the boot order to be changed in the BIOS and this should be allowed under the defined security policy of the organization (OP.CLEAN)

OE.PROPER_USE

This concerns with the trustworthiness of the users of the TOE. The TOE cannot enforce by technical means that only sound operation of the TOE is carried out. Therefore, it must be

assumed that the user of the TOE is not malicious and does not intentionally attempt to abuse or misuse the TOE, and at all times follows the guidance of the TOE. This is addressed by assumption A.PROPER_USE in the operational environment of the TOE. The organization using the TOE must also define and enforce a policy on whether reports in PDF are allowed when the reports are stored locally (OP.PDF). Also a policy on how to properly handle RAID disks must also be defined and put into effect(OP.RAID).

The user should use the TOE as given in the Guidance document titled **BitRaser Drive Eraser – User Guide ver 3.0**. The GUI runs locally on the same host as the **BitRaser Drive Eraser** application.

Users of the TOE are not careless, willfully negligent, or hostile and will follow the Guidance document

4.3. Security Objectives Rationale

4.3.1. Tracing of Security Objectives

The following table provides the tracing of the security objectives to the threats, organizational security policies, and assumptions:

	O.COMPLETE_ERASURE	O.LEGIT_USE	OE.PLATFORM	OE.PROPER_USE
T.INCOMPLETE_ERASURE	X			
T.UNAUTH_USER		X		
OP.ERASE	X			
OP.RAID				X
OP.PDF				X
OP.CLEAN			X	
A.PLATFORM			X	
A.PROPER_USE		X		X

4.3.2. Justification of the Tracing

O.COMPLETE_ERASURE concerns with ensuring that upon completion of a drive erasure either the drive is fully erased in accordance with the selected erasure standard or the user

of the TOE is provided with a reliable indication that the erasure was unsuccessful. The TOE implements a number of different erasure standards and the erasure is only sufficient if

1. The erasure standard selected, fulfills the secure erasure objectives as defined under the media erasing policy (OP.ERASE) of the organization using the TOE.
2. The erasure is completed in accordance with the selected erasure standard.
3. The erasure is complete or the user is given an unambiguous notification of the failure.

Concern #1 is addressed if the organization using the TOE ensures the sufficient policies for erasure are defined. This is addressed if OP.ERASE is defined and enforced. Concern #2 is addressed if threat T.INCOMPLETE_ERASURE is prevented from occurring.

O.LEGIT_USE concerns with ensuring that the TOE is only used in a legitimate manner and by the legitimate users. To ensure this, the TOE implements technical countermeasures for protecting itself from interference but also requires the organization using the TOE to ensure that the policies governing the use of the TOE and the level of acceptable risk when using the TOE are considered (A.PROPER_USE). Also, the concern regarding legitimate users can be handled by avoiding T.UNAUTH_USER to occur.

OE.PLATFORM concerns with acknowledging that the TOE is application level software that requires on the underlying platform for execution and that there is a risk that the underlying platform is also running software attempting to prevent the TOE from achieving its security objectives. To fulfill this objective for the environment for the TOE, the organization using the TOE must

1. Acknowledge the possibility of malicious processes being executed in the underlying platform.
2. Assess the risk of malicious processes and define the minimum criteria for the trustworthiness of the platforms on which only the TOE may be used.

Concern #1 is addressed by assumption A.PLATFORM and concern #2 is addressed by the organization using the TOE, by defining and enforcing policy OP.CLEAN.

OE.PROPER_USE concerns with the trustworthiness of the users of the TOE. The TOE cannot enforce, by technical means, that only sound operation of the TOE is carried out.

Therefore, it must be assumed that the user of the TOE is not malicious and does not intentionally attempt to abuse or misuse the TOE, and at all times follows the guidance of the TOE. This is addressed by assumption A.PROPER_USE in the operational environment of the TOE. The organization using the TOE must also define and enforce a policy on whether reports in PDF are allowed when the reports are stored locally (OP.PDF), how to properly handle RAID disks (OP.RAID).

5. EXTENDED COMPONENT DEFINITION

This ST defines no extended components applicable to the TOE. Therefore, this section is not applicable and is omitted.

6. SECURITY REQUIREMENTS

This section defines the security requirements for the TOE. The security functional requirements are defined with reference to CC Part 2 and Sect. 6. The security assurance requirements are defined with reference to a well-defined evaluation assurance package EAL2 defined in CC Part 3. The ST claims no extensions or augmentations to the package EAL2.

The statement of security functional requirements utilizes operations as defined for each applicable security functional requirement in CC Part 2 and Sect. 6. The notation for identifying the operations is given as follows:

Iteration is identified by repeating the identifier of the security functional requirement with a string indicating a specific iteration separated from the SFR identification by a slash (e.g. FCS_COP.1/AES, FCS_COP.1/DSIG).

Refinement is identified by **a)** Indicating in square brackets in bold font any added text, in form of [Refinement: added text] and **b)** Indicating any removed words using ~~overstrike~~ font. Whenever a refinement is used, the rationale and justification of the refinement are given immediately after the statement of the security requirement.

Selection is identified by indicating the selected values in [square brackets using **bold** font].

Assignment is identified by indicating the assigned values in [*square brackets using **bold**, italic font*].

Application notes may be added after the formal statement of the security requirements to help the user understand the specific security requirement in the context of this particular TOE.

6.1. Statement of Security Functional Requirements

6.1.1. Class FCS: Cryptographic Support

6.1.1.1. FCS_COP.1 Cryptographic operation

FCS_COP.1.1 The TSF shall perform **[*cryptographic operations stated in Table below*]** in accordance with a specified cryptographic algorithm **[*stated in Table below*]** and cryptographic key sizes **[*stated in Table below*]** that meet the following: **[*stated in Table below*]**.

Operation	Key Generation	Key Destruction	Algorithm	Key Size	Standard
Computing MD5 value for erasure report to create digital identifier of report	NA	NA	MD5	NA	RFC 1321
Encrypting/Decrypting USB licenses	NA	NA	AES	128 bit	FIPS PUB 197

Application note: The cryptographic operations use keys embedded into the ISO image during the manufacturing of the TOE. These keys can neither be changed nor destroyed by the TOE.

6.1.2. Class FDP: User Data Protection

6.1.2.1. 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 [**refinement:** assured by the TOE] is made unavailable upon [deallocation of the resource from] the following objects: [BitRaser Drive Eraser].

Application Note: The resource (storage device) is allocated to the TOE for erasure using the method selected by the user of the TOE. The previous information content of the resource will be made unavailable when the resource is deallocated from the TOE.

6.1.3. Class FIA: Identification and Authentication

6.1.3.1. FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note: The user is identified through the licenses held by the user. All operations require a license.

6.1.4. Class FPT: Protection of the TSF

6.1.4.1. FPT_TEE.1: Testing of external entities

FPT_TEE.1.1 The TSF shall run a suite of tests **[on the storage drive after each round of erasure, during which verification is done by reading the pattern in each of the sectors and matching it with the expected pattern as per the selected erasure algorithm]** to check the fulfillment of **[complete erasure of the drive].**

FPT_TEE.1.2 If the test fails, the TSF shall **[*Report to the user*].**

Application note: Verification of the erasure is performed after each round of erasure. During the Erasure process the TOE verifies the sectors of the storage device and validates if it has been overwritten. This verification is done by reading the pattern in the sector and matching it with the expected pattern as per the selected erasure algorithm. Failure to read the pattern or pattern mismatch means failure of the test.

6.1.5. Class FAU: Security Audit

6.1.5.1. FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable Time Stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

[

- **Start-up and shutdown of the audit functions;**
- **All auditable events for the [not specified] level of audit; and**

- **[assignment: Erasure events]**

].

Application Note: A media erasure report is created by the TOE that will include information about the erasure of the hard drive (as defined in this section under FAU_GEN.1.2).

Application Note: System time is provided by the BIOS hardware clock.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

[

- **Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event;**
- **For each audit event type, based on the auditable event definitions of the functional components included in the ST.**
- **[BitRaser Drive Eraser version number, drive model information, serial number of physical drive, current user (user-defined, name of person performing the Eraser), computer ID (user-defined, name of the drive or system), type of operation performed (user definable erasure pattern), number of overwrites performed, date and time operation was completed, total elapsed time, operation result, the total number of disk sector read/write errors, if any; total uncleaned or unreadable disk sectors, if any; number of Erase passes, NIST Method type, if applicable; drive type (e.g. Platter, SSD)]**

].

6.2. Statement of Security Assurance Requirements

Security assurance requirements for the TOE constitute the evaluation assurance package EAL2 and are fully defined with reference to CC Part 3. The security assurance requirements constituting EAL2 are the following:

- Assurance Class ADV: Development
  - ADV_ARC.1 Security architecture description
  - ADV_FSP.2 Security-enforcing functional specification
  - ADV_TDS.1 Basic design
- Assurance Class AGD: Guidance documents
  - AGD_OPE.1 Operational user guidance
  - AGD_PRE.1 Preparative procedures
- Assurance Class ALC: Life-cycle support
  - ALC_CMC.2 Use of a CM system
  - ALC_CMS.2 Parts of the TOE CM coverage
  - ALC_DEL.1 Delivery procedures
- Assurance Class 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
- Assurance Class ATE: Tests
  - ATE_COV.1 Evidence of coverage
  - ATE_FUN.1 Functional testing

- ATE_IND.2 Independent testing – sample

- Assurance Class AVA: Vulnerability assessment
  - AVA_VAN.2 Vulnerability analysis

6.3. Security Requirements Rationale

6.3.1. Security Requirement Dependency Rationale

Each dependency of SFRs defined for the TOE is satisfied by the TOE. The satisfaction of dependencies for each SFR is given in the table below

SFR	Dependencies	Justification
FCS_COP.1	FCS_CKM.1, FCS_CKM.4	The TOE implements cryptographic operations that use static keys that are part of the ISO image and cannot be created, changed, or destroyed. For these keys, none of the dependencies are applicable. Some Encryption functions are hash functions that require no keys. FCS_CKM.1, FCS_CKM.4 are not applicable as the keys are neither generated nor destroyed.
FDP_RIP.1	No dependencies	Not applicable
FIA_UID.2	No dependencies	Not applicable
FPT_TEE.1	No dependencies	Not applicable
FAU_GEN.1	FPT_STM.1	The TSF shall be able to generate an audit record of the start-up and shutdown of the audit functions. FPT_STM.1 is dependent on the TOE environment.

6.3.2. Tracing of Security Objectives to Security Functional Requirements

The following table provides the tracing of security objectives to the security functional requirements:

SFR	O.COMPLETE_ERASURE	O.LEGIT_USE	OE.PLATFORM	OE.PROPER_USE
FCS_COP.1		X		
FDP_RIP.1	X			
FIA_UID.2		X		
FPT_TEE.1	X			
FAU_GEN.1	X			

O.COMPLETE_ERASURE concerns with ensuring that upon successful completion of a drive erasure, either the drive is fully erased in accordance with the selected erasure method, or the user of the TOE is provided with a reliable indication that the erasure was unsuccessful. The TOE implements several different erasure methods and ensures that the selected drive is erased in accordance with the selected method (FDP_RIP.1). Upon completion of the erasure, the TOE also verifies the erasure outcome to ensure the completeness of the erasure and the user of the TOE is notified of any discrepancy (FPT_TEE.1). This report can be referred to at a later stage for the purpose of auditing as well (FAU_GEN.1).

O.LEGIT_USE concerns with ensuring that the TOE is only used legitimately and that the sufficient countermeasures ensure that the behavior of the TOE cannot be falsified by malicious agents. While the prevention of malicious processes from falsifying the erasure results is largely a policy concern, the TOE does implement encryption on the license data stored in the USB lock key. Also, the TOE attaches a digital identifier with the erasure report. The digital identifier is generated using the encrypted data of the erasure operation(FCS_COP.1).

The TOE ensures that each access request is investigated and only the legitimate ones are allowed. For each request, the licenses of the user are examined, and the operation is only

granted if the available licenses match the license required for the operation. By default, any operation is disallowed unless sufficient licenses are available and the TOE cannot be configured to allow operations if licenses are not present. Users are identified through the licenses and a license is required for each operation (FIA_UID.2).

6.3.3. Justification for the Security Assurance Requirements

The Security Assurance Requirements selected for the TOE constitute a well-defined evaluation assurance package EAL2 and as such, are an internally consistent set of security assurance requirements.

7. TOE SUMMARY SPECIFICATION

An explanation of how the TOE meets the Security Functional Requirements at the level of detail suitable for the TOE Summary Specification is given in Table below:

SFR	**Justification**
FCS_COP.1	The erasure reports contain a digital identifier generated by MD5 hashing process of encrypted report data. The MD5 key used for the digital identifier is generated after erasing process by the TOE and cannot be re-generated, changed, or destroyed by the TOE. When stored on a USB lock key, the licenses are encrypted with a 128-bit AES key, generated and stored on the TOE during the production of the TOE. That key cannot be created, modified, or destroyed by the TOE but can be used for decrypting the licenses fetched from a USB lock key for the TSF.
FDP_RIP.1 FPT_TEE.1	When the TOE is running in the Host PC, TOE provides a list of all drives connected to the Host PC to the user. The user may select any of the drives and any of the available erasure methods to trigger the execution of the erasure. The TOE executes the selected erasure algorithm on the selected drive. During the erasure, the TOE displays the status of the erasure of each drive to the user. The status of each drive erasure is displayed in the Drive's Progress Bar and in percentage. The status may be Running, Stopped, Failed, or Completed. Status Completed implies successful completion of the erasure. There is, however, a possibility of a malfunctioning drive firmware signaling successful erasure when the erasure was not complete. To ensure a dependable outcome of the erasure, the TOE verifies the erasure outcome before reporting to the user. If for any reason the verification result is negative, the TOE shall report that the erasure Failed.
FIA_UID.2	The TOE does not operate on the actual identities of users. Instead, each user is identified by the set of licenses they possess. The possession of licenses is used in determining whether a user is granted access to execute requested functions of TOE or not. Each operation requires an erasure license.
FAU_GEN.1	TOE generates auditable data of the start-up and shutdown of the audit functions.