Indian CC Certification Scheme (IC3S)

Certification Report

Report Number	**:**	**STQC/ IC3S/KOL01/STELLAR/EAL2/0221/0028/CR**
Product / system	:	**BitRaser Drive Eraser V3.0.0.6**

Dated: 20th November 2023

Version: 1.0

Government of India
Ministry of Electronics & Information Technology
Standardization Testing and Quality Certification Directorate
6. CGO Complex, Lodi Road, New Delhi –
110003 India

This report contains a total of 15 pages. In case it needs to be reproduced, all the pages must be included.

Product developer:	Stellar Information Technology Private Ltd. D-16, INFOCITY PHASE-2, SECTOR-33, GURUGRAM, HARYANA-122001
TOE evaluation sponsored by:	Stellar Information Technology Private Ltd. D-16, INFOCITY PHASE-2, SECTOR-33, GURUGRAM, HARYANA-122001
Evaluation facility:	**Common Criteria Test Laboratory**, **ERTL (East**), 63 DN-Block, Sector V, Salt Lake, Kolkata-700091, India.
Evaluation Personnel:	**Evaluators:** Malabika Ghose **Test engineers:** Nischal, Aniruddha Ghosh, Avishek Raychoudhury
Evaluation report:	IC3S/KOL01/STELLAR/EAL2/0221/0028/ETR/0046
Validation Personnel:	A K Upadhyaya, Scientist G, STQC, Govt. of India

Table of Contents

Contents

PART A: CERTIFICATION STATEMENT AND BACKGROUND OF THE CERTIFICATION BODY

A1 Certification Statement

The product below has been evaluated under the terms of the Indian Common Criteria Certification Scheme (IC3S) and has met the stated Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.	
Sponsor	Stellar Information Technology Private Ltd. D-16, INFOCITY PHASE-2, SECTOR-33, GURUGRAM, HARYANA-122001
Developer	Stellar Information Technology Private Ltd. D-16, INFOCITY PHASE-2, SECTOR-33, GURUGRAM, HARYANA-122001
The Target of Evaluation (TOE)	BitRaser Drive Eraser V3.0.0.6
Security Target	BitRaser Drive Eraser V3.0.0.6
Brief description of product	BitRaser Drive Eraser is developed by Stellar Information Technology. It 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.
Common Criteria Standard	Common Criteria Standard Version 3.1 Revision 5
CC Part 2 [CC-II]	Conformant
CC Part 3 [CC-III]	Conformant
EAL	EAL2
Evaluation Lab	Common Criteria Test Laboratory, ERTL(E), Kolkata, India
Date Authorized	16th February 2021

A2. About the Certification Body

STQC IT Certification Services, the IT Certification Body of Standardization Testing and Quality Certification – was established in 1998 and offers a variety of services in the context of security evaluation and validation. It is the first Certification Body in India for BS 7799/ISO 27001 certification of Information Security Management Systems (ISMS). The Indian CC Certification Scheme (IC3S) is the IT security evaluation & certification Scheme based on Common Criteria standards, it is established by Govt. of India under Department of Information Technology, STQC Directorate to evaluate & certify the trustworthiness of security features in Information Technology (IT) products and systems. The IC3S is an Indian independent third party evaluation and certification scheme for evaluating the security functions or mechanisms of the IT products. It also provides framework for the International Mutual Recognition of such certificates with the member countries of CCRA (Arrangement on the Recognition of Common Criteria Certificates in the field of

Information Technology Security). The principal participants in the scheme are:

a) Applicant (Sponsor/Developer) of IT security evaluations;

b) STQC Certification Body (STQC/MeitY/Govt. of India);

c) Common Criteria Testing Laboratories (CCTLs).

A3 Specifications of the Certification Procedure

The certification body operates under the official administrative procedures according to the criteria and procedures laid down in the following:

- ISO/IEC Guide 65, and the requirements laid down in Annex C of CCRA
- Indian Common Certification Scheme (IC3S)
- STQC/CC/DO2: Standard Operating Procedure (SOP) for Certification Body - Quality Manual – describes the quality management system for the Scheme.
- Common Criteria for Information Technology Security Evaluation (CC) part 1-3, Version 3.1, Revision 5
- Common Evaluation Methodology (CEM) Version 3.1., Revision 5

A4 Process of Evaluation and Certification

The certification body monitors each individual evaluation to ensure uniform procedures, interpretations of the criteria, and ratings. The TOE has undergone the certification procedure at **STQC IT Certification Body**. The evaluation of the product was conducted by the evaluation body Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. Hereafter this has been referred as CCTL. The evaluation facility is recognized under the IC3S scheme of STQC IT Certification Body.

Stellar Information Technology Private Ltd. D-16, INFOCITY PHASE-2, SECTOR-33, GURUGRAM, HARYANA-122001 is the developer and sponsor of the TOE evaluation.

The certification process is concluded with the completion of this certification report.

This evaluation was completed on **04th October 2023** after submission of [**ETR**] to the certification body. The confirmation of the evaluation assurance level (EAL) only applies on the condition that

- all stated condition regarding configuration and operation, as given in part B of this report, are observed,
- The product is operated – where indicated – in the operating environment described.

This certification report applies only to the version and release of the product indicated here. The validity of the certificate can be extended to cover new versions and releases of the product, provided the applicant applies for re-certification of the modified product, in accordance with the procedural requirements, and provided the evaluation does not reveal any security deficiencies.

A5 Publication

The following Certification Results consist of Sections B1 to B11 of this report. The TOE will be included in the list of the products certified under IC3S Scheme of STQC IT Certification Body. The list of certified products is published at regular intervals in the Internet at http://www.commoncriteria-india.gov.in. Further copies of this certification report may be ordered from the sponsor of the product. The certification report may also be obtained in electronic form on request to the Certification Body.

PART B: CERTIFICATION RESULTS

B.1 Executive Summary

B.1.1 Introduction

The Certification Report documents the outcome of Common Criteria security evaluation of the TOE. It presents the evaluation results and the conformance results. This certificate is intended to assist the prospective buyers and users when judging the suitability of the IT security of the product for specified requirements.

Prospective buyers and users are advised to read this report in conjunction with the referred [ST] of the product, which specifies the functional, environmental and assurance requirements.

The evaluation was performed by Common Criteria Test Laboratory (CCTL), ERTL (East), DN Block, Sector V, Salt Lake, Kolkata-700091, India. The information in the test report is derived from the [ST] written by the developer and the Evaluation Technical Report [ETR] written by Common Criteria Test Laboratory [CCTL, ERTL (E)], ERTL (EAST), Block-DN Sector-V, Kolkata, India. The evaluation team determined the product to be CC Version 3.1, Part 2 and Part 3 conformant and concluded that the Common Criteria requirements for Evaluation Assurance Level (**EAL 2**) have been met.

B 1.2 Evaluated product and TOE

The TOE consists of BitRaser Drive Eraser V3.0.0.6 software which is contained in a bootable ISO. TOE with the USB lock key has been considered for the purpose of evaluation

SHA256 of BitRaser Drive Eraser V3.0.0.6 software: da50dbca9b964bb294b37539d50c4511b5 e6794096878a5a0dd8595b3e2483f3

The evaluated sub-set and configuration of the product is described in this report as the Target of Evaluation (TOE). The Evaluated Configuration, its security functions, assumed environment, architectural information and evaluated configuration are given below (Refer B2 to B5).

B 1.3 Security Claims

The [ST] specifies the security objectives of the TOE and the threats that they counter (Refer 3.3 and 4.1 of ST). All the Security Functional Requirements (SFRs) (listed in 6.1 of ST) are taken from CC Part 2 are included.

B 1.4 Conduct of Evaluation

The evaluation was initiated by the IC3S Certification Scheme of STQC IT Certification Body vide communication no. IC3S/CB/2021/0030 dated 12th February 2021.

The TOE as described in the [ST] is BitRaser Drive Eraser V3.0.0.6 software which is contained in a bootable ISO. The TOE was evaluated through evaluation of its documentation; testing and vulnerability assessment using methodology stated in Common Evaluation Methodology [CEM] and Common Criteria Test Laboratory, ERTL (E), Kolkata, Operating Procedure OP-07(CC EAL 4).

The evaluation has been carried out under written agreement [26th February 2021] between Common Criteria Test Laboratory, ERTL (E), Kolkata and the sponsor.

B 1.5 Independence of Certifier

The certifier did not render any consulting or other services for the company ordering the certification and there was no relationship between them, which might have an influence on this assessment.

B 1.6 Disclaimers

The certification results only apply to the version and release of the product as indicated in the certificate. The certificate is valid for stated conditions as detailed in this report. This certificate is not an endorsement of the IT product by the Certification Body or any other organization that recognizes or gives effect to this certificate. It is also not an endorsement of the target of evaluation (TOE) by any agency of the Government of India and no warranty of the TOE is either expressed or implied.

B 1.7 Recommendations and conclusions

- The conclusions of the Certification Body are summarized in the Certification Statement at Section A1.
- The specific scope of certification should be clearly understood by reading this report along with the [ST].
- The TOE should be used in accordance with the environmental assumptions mentioned in the [ST].
- The TOE should be used in accordance with the supporting guidance documentation.
- This Certification report is only valid for the evaluated configurations of the TOE.

B2 Identification of TOE

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.

Table 1: TOE and Non-ToE Components

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.

B2.1 Deliverables to be provided by the Developer to the End-user:

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.

- Operation User Guidance /configuration documents title: BitRaser Drive Eraser – User Guide for TOE version 3.0.0.6

B3 Security policy

There are following organizational security policies that the TOE must meet (Given in table 2 below).

Table 2: Organizational Security Policies

Security Policy Code	Description
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.
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.

B.4 Assumptions

There are following assumptions exist in the TOE environment.

Table 3: Assumptions

Assumption	Description
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.

B.5 Evaluated configuration

The TOE is executable software inside the bootable ISO image. 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 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. The following table provides the Details of evaluated configuration of the TOE:

Table 4: Details of evaluated configuration of the TOE

Description	Software Version and Release	The image files	File size in bytes	Hash values of the image files
Bitraser ISO file containing TOE	Version 3.0.0.6	BITRASER-2023.07.28-x86_64.iso	789504 KB	MD5: 8e3739c464f2d2094d8044cd7f6425e5 SHA256: ff30e63264822f06dca1eb39d3a6f10cabe4e375a339964ed795701b2f5dec25
TOE contained inside Bitraser	Version 3.0.0.6	Bitraser (ELF 64 bit executable file)	20857.9 KB	MD5: 008bcaa965acfd05034f577d3c4e1b92 SHA256: da50dbca9b964bb294b37539d50c4511b5e6794096878a5a0dd8595b3e2483f3

B6 Document Evaluation

B.6.1 Documentation

The list of documents, those were presented, as evaluation evidences to the evaluators at the evaluation facility, are given below:

1. **Security Target**: BitRaser Drive Eraser Version 3.0.0.6 Security Target, Version 1.1,
2. **TOE Architecture:** Security Architecture Description Document, Version 1.0
3. **TOE Functional Specification:** BitRaser Drive Eraser Version 3.0.0.6 Functional Specification Document,

Version 1.0

4. **TOE Design description**: BitRaser Drive Eraser Version 3.0.0.6 Design Document Version 1.0
5. **Preparative Guidance**: BITRASER Drive Eraser User Guidance for version 3.0.0.6
6. **Operational Guidance**: BITRASER Drive Eraser User Guidance for version 3.0.0.6
7. **Configuration Management Capability:** CMC Document, Version 1.0
8. **Configuration Management Scope:** CM Scope Document, Version 1.0
9. **TOE delivery:** Delivery Document, Version 1.0
10. **Test cases, logs and coverage**: Functional Testing Document, Version 1.0

B.6.2 Analysis of document

The documents related to the following areas were analyzed using [CEM]. The summary of analysis is as below:

Development process: The evaluators analyzed the functional specification of the TOE and found that the TOE security function interfaces are described clearly and unambiguously. The evaluators also analyzed design and architectural descriptions of the TOE and determined that the TOE (BitRaser Drive Eraser V3.0.0.6 software) is clearly described in the design description. The evaluators determined that architectural description of the TOE includes secure initialization and license determination of the TOE and also means of protection of the TOE from tampering and bypassing.

Guidance Documents: The evaluators analysed guidance documents like preparative procedure and operational user guidance and determined that preparative procedure describes clear and unambiguous steps to bring the TOE to its secure state. The operational user guidance information were also clear and unambiguous.

Life-cycle support documents: The Life cycle support process document, containing information on Configuration Management and Delivery Procedure were evaluated.

Configuration management: The evaluators analyzed configuration management documentation and determined that the TOE and its associated documents are clearly identified as configurable items. The evaluators also analyzed access control measures defined in the documentation and found satisfactory**.**

Delivery procedure: The delivery procedure document was audited with the objective to ascertain whether it covers secure delivery of the TOE to the end-users. The secure delivery procedure has been described in the document and the same has been audited by the evaluators during their virtual site visit. The end-users can check integrity of the evaluated TOE using hash value of that, if felt necessary.

The final version of the respective evaluation evidences was found to comply with the requirements of CC v3.1 for EAL2.

B7 Product Testing

Testing at EAL2 consists of the following three steps: Testing by developer, Independent Testing by Evaluation Team, and Penetration testing.

B 7.1 IT Product Testing by Developer

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the [ETR].

The evaluators analysed the developer’s test coverage and found them to be complete and satisfactory. The correspondence between the tests identified in the developer’s test documentation and the functional specification and TOE design was complete.

B 7.2 IT Product Independent Testing by Evaluation Team

The evaluators' independent functional testing effort is summarized as below.
All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and reproducibility of results.

The TOE has been installed properly as per the preparative procedure document.
The evaluators have repeated the developer's test at CCTL, ERTL(E), Kolkata to confirm the reproducibility of the test results.
While making the test strategy for independent testing, consideration is given to cover the security requirements, as well as the security specification as defined in the security target, interfaces available to the users to cover each of security functional requirements, TOE design and security architecture information. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.

The evaluators test effort is summarized as below:

#	Aspects	Evaluator's comments
1	On overall evaluator testing strategy &approach	The evaluators simulated all of the developers' tests and found that those are reproducible; in addition to that they developed test cases that augment the developer tests and conducted most of those cases independently at CCTL, Kolkata.
2	On TOE test configurations: The particular configurations of the TOE that were tested, including whether any privileged code were required to set up the test or clean up afterwards.	The evaluators have examined the TOE and it was found to be configurable as per the description given in the developer's preparative guidance document. It is also observed that the test configuration is consistent with the description as given in the security target document. The TOE was installed properly as per the preparative procedure AGD_PRE document.
3	On depth of testing in respect of all functionalities of all TSFs	The evaluators have repeated all the test objectives of developer's tests at CCTL, Kolkata to verify the reproducibility of test results and to ensure the coverage of all TSFIs, as mentioned in the FSP document. In addition to that they developed test cases that augment the developer tests and conducted most of those cases independently at CCTL, Kolkata. Highlights of Independent testing are given below: • The TOE was installed properly as per the preparative procedure AGD_PRE document. • The evaluators have repeated the developer's test at CCTL, Kolkata to confirm the reproducibility of the test results.

		While making the test strategy for independent testing, consideration is given to cover the security requirements as defined in the security target, visible interfaces available to the users to cover each of security functional requirements, TOE design information and its security architecture. Independent testing is designed to verify the correct implementation of security functionalities available to different levels of users and to check whether audit is being generated for auditable events.
4	On test results: A description of the overall evaluator testing results	The evaluator conducted tests on the TOE executable delivered by the developer and found to be in compliance with the ST. Moreover, snapshots of code snippets are analyzed to ascertain erasure algorithms implementation as per requirements of standards.

B 7.3 Vulnerability Analysis and Penetration testing

Evaluators searched over internet for potential vulnerabilities of BitRaser. No vulnerabilities could be found from public domain for the TOE due to following reasons:

- No external interfaces with IP addresses or network-level access in Bitraser Application is available.
- No vulnerabilities were reported in Bitraser Drive Erasure of Stellar till date.

The TOE documents like, Security Target (ST), TOE architecture & Design (TDS), TOE Preparatory guidance document etc. were analysed to find out potential security vulnerabilities and the same is listed out.

The attack potential for each of the vulnerabilities was calculated using guidance given in CEMv3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

Considering the type of the TOE and its intended use, the possibility of “Direct Attack” is negligible; evaluator’s judgement is justified and supported by analysis. The evaluator has identified the following Attack scenarios.

AT1: An adversary attempts to tamper with a report by forging meaningful data, comprising well-defined English words and numerals, in order to produce an identical digital identifier as that of a genuine erasure report.

AT2: An attacker attempts to retrieve data from a USB drive that was previously erased using Bitraser drive erasure software. He conducts a Direct Attack on the data erasure mechanism, utilizing standard forensic tools like Autopsy to assess if the old files can be retrieved.

AT3: Attacker will try to retrieve old data using hexviewer or Autopsy tool (as shown in PT1) from previously erased media by directly attacking the implementation of srand() and rand() in NIST Clear, which may render the TSF vulnerable.

AT4: An Attacker, when presented with the absence of an encrypted license count or the presence of an unencrypted one, gains the capability to initiate a Monitoring Attack. This enables the attacker to execute the BITRASER application without license or manipulate the lock count variable at will.

The attack potential for each of the vulnerabilities was calculated using guidance given in CEM v3.1 and considering various factors like the time to identify & exploit the vulnerability, expertise required, knowledge of the TOE, windows of opportunity and equipment requirement.

The relevant attack potentials, corresponding to the identified vulnerabilities have been estimated considering various factors like the 'time to identify & exploit', 'expertise required', 'knowledge of the TOE', 'windows of opportunity' and 'equipment required'. The potential vulnerabilities with '**Basic**' attack potential were considered for penetration testing. The calculated attack potentials are as follows:

AT1. Attack Potential: 8 (Within Basic)
AT2. Attack Potential: 7 (Within Basic)
AT3. Attack Potential: 8 (Within Basic)
AT4. Attack Potential: 8 (Within Basic)

The evaluator conducted Penetration Testing (PT1, PT2, PT3 and PT4 respectively) for AT1, AT2, AT3 and AT4 and could not able to exploit the hypothesized Security vulnerabilities of the TOE evolved through analysis of evaluation objects.

Hence, it is concluded that the TOE does not contain any exploitable vulnerability for 'Basic Attack Potential'.

B 8 Evaluation Results

The evaluation results have been documented in the [ETR].

Report No: IC3S/KOL01/STELLAR/EAL2/0221/0028/ETR/0046

The TOE was evaluated through evaluation of its documentation, testing and vulnerability assessment using methodology stated in [CEM] and laboratory operative procedure [OP-07 CC EAL 4].

Documentation evaluation results:

The documents for TOE and its development life cycle were analyzed by the evaluator in view of the requirements of the respective work units of the [CEM]. The final versions of the documents were found to comply with the requirements of CC version 3.1 Revision 5 for EAL 2.

Testing:

The developer's tests and the independent functional tests yielded the expected results, giving assurance that '**BitRaser Drive Eraser V3.0.0.6'**, behaves as specified in its [ST], functional specification and TOE design.

Vulnerability assessment and penetration testing:

The penetration testing with '**Basic**' attack potential could not exploit the potential vulnerabilities identified through vulnerability assessment.

B 9 Validator Comments

The Validators have reviewed the Evaluation Technical Report [ETR] along with all relevant evaluation evidences, documents, records, etc. and are in agreement with the conclusion made in it i.e.

- **The [ST] BitRaser Drive Eraser Version 3.0.0.6 Security Target, Version 1.1 has satisfied all the requirements of the assurance class ASE.**
- **The results of evaluation of product and process documentation, testing and vulnerability assessment confirm that BitRaser Drive Eraser V3.0.0.6, satisfies all the security functional requirements and assurance requirements as defined in the [ST]. Hence, the TOE is recommended for EAL2 Certification**.

However, it should be noted that there are no **Protection Profile** compliance claims.

B 10 List of Acronyms

ACL: Access Control List

CC: Common Criteria

CCTL: Common Criteria Test Laboratory CEM: Common Evaluation Methodology DVS: Development security

EAL: Evaluation Assurance Level ETR: Evaluation Technical Report FSP: Functional Specification

IC3S: Indian Common Criteria Certification Scheme

IT: Information Technology

PP: Protection Profile ST: Security Target

TOE: Target of Evaluation

TDS: TOE Design Specification

TSF: TOE Security Function

TSFI: TOE Security Function Interface

B 11 References

1. [CC-I]: Common Criteria for Information Technology Security Evaluation: Part 1: Version 3.1
2. [CC-II]: Common Criteria for Information Technology Security Evaluation: Part 2: Version 3.1, Revision 5
3. [CC-III]: Common Criteria for Information Technology Security Evaluation: Part 3: Version 3.1 Revision 5
4. [CEM]: Common Methodology for Information Methodology: Version 3.1 Revision 5
5. [ST]: BitRaser Drive Eraser Version 3.0.0.6 Security Target, Version 1.1
6. [ETR]: Evaluation Technical Report No. Report No: IC3S/KOL01/STELLAR/EAL2/0221/0028/ETR/0046 version 1.0
7. [OP-07 CC EAL 4]: CCTL, ERTL(E) Operating procedure, Issue no. 8.0