Certificate Report

Version 1.0

12 August 2021

CSA_CC_20006

For

Securaze-Engine
Version 2.0

From

Securaze AG

This page is left blank intentionally

Foreword

Singapore is a Common Criteria Certificate Authorizing Nation, under the Common Criteria Recognition Arrangement (CCRA). The current list of signatory nations and approved certification schemes can be found at the CCRA portal:

https://www.commoncriteriaportal.org

The Singapore Common Criteria Scheme (SCCS) is established for the info-communications technology (ICT) industry to evaluate and certify their IT products against the requirements of the Common Criteria for Information Technology Security Evaluation (CC), Version 3.1 (ISO/IEC 15408) and Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 (ISO/IEC 18045) in Singapore.

The SCCS is owned and managed by the Certification Body (CB) under the ambit of Cyber Security Agency of Singapore (CSA).

The SCCS certification signifies that the target of evaluation (TOE) under evaluation has been assessed and found to provide the specified IT security assurance. However, certification does not guarantee absolute security and should always be read with the particular set of threats sought to be addressed and assumptions made in the process of evaluation.

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
1.0	August 2021	Released

NOTICE

The Cyber Security Agency of Singapore makes no warranty of any kind with regard to this material and shall not be liable for errors contained herein or for incidental or consequential damages in connection with the use of this material.

Executive Summary

This report is intended to assist the end-user of the product in determining the suitability of the product in their deployed environment.

The Target of Evaluation (TOE) is the Securaze Eraser Engine version 2.0 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS).

The TOE consists of the following.

Name and version	Version
Securaze-Engine	2.0

Table 1 - TOE components identifier

The list of guidance documents to use with the product in its certified configuration is as follows:

Name and version	Version
Manual [1]	1.0.0
Work [2]	2.3.0
Mobile [3]	2.0.0

Table 2 - List of guidance documents

The Securaze Software Suite includes the Securaze Work (software tool for erasure of HDD/SSD), Securaze Mobile (software tool for erasure of mobile devices) and the Securaze Dashboard (web user interface to install Securaze Work or to download Securaze Mobile).

The Securaze Engine (i.e. the TOE) is a software engine that is embedded within and acts as a client library that provides erasure functionality to the Securaze Work and Securaze Mobile.

The evaluation of the TOE has been carried out by An Security, an approved CC test laboratory, at the assurance level CC EAL 2 and was completed on 10 August 2021.

The certification body monitored each evaluation to ensure a harmonised procedure and interpretation of the criteria has been applied.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality
Performing erasure of data by overwriting the data using a defined algorithm.
Generation of audit records for the result of the erasure process.

Table 3: TOE Security Functionality

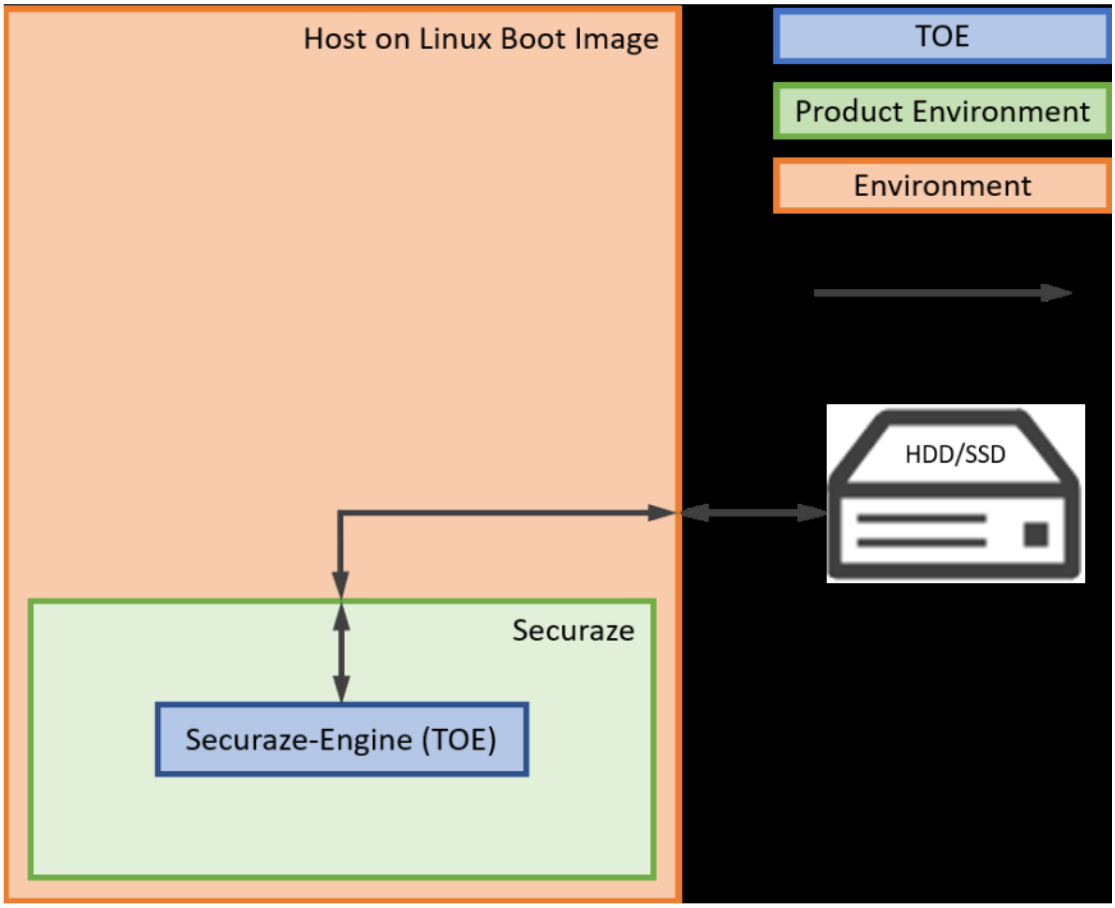

Figure 1 - Overview of Securaze Work

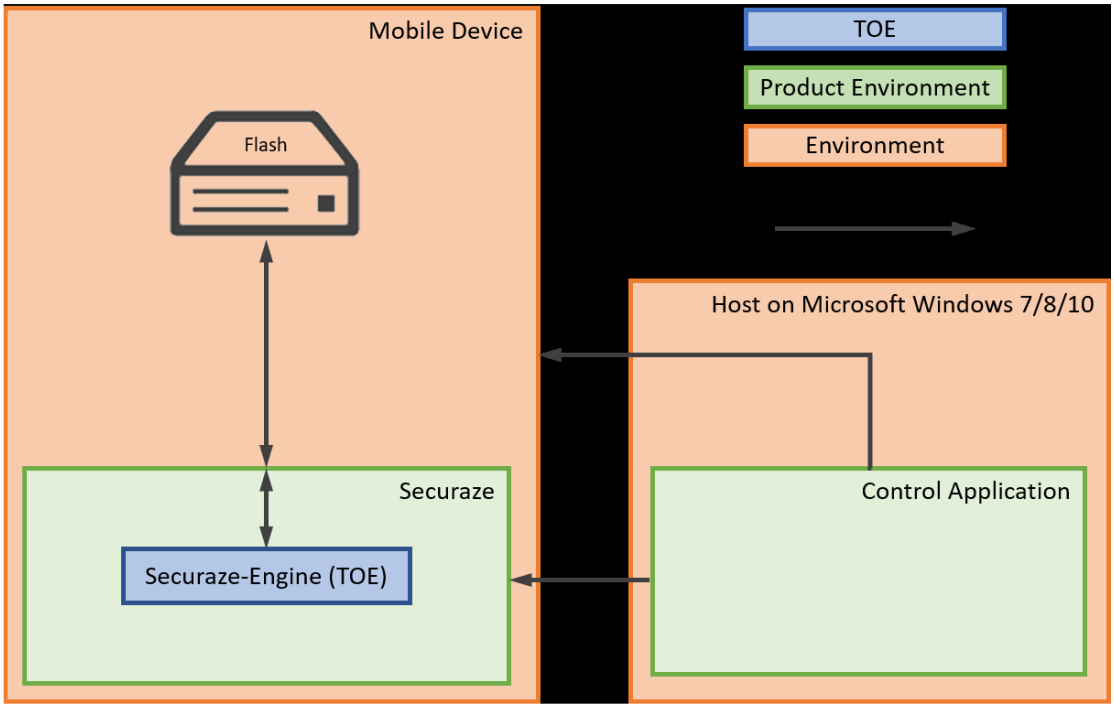

Figure 2 - Overview of Securaze Mobile

Please refer to the Security Target [4] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target [4]

This Certification covers the configurations of the TOE as outlined in Chapter 5.3 of this report.

The certification results only apply to the version of the product indicated in the certificate and on the condition that it is in compliance with all the stipulations as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration.

Table of Contents

1 Certification

1.1 Procedure

The certification body conducts the certification procedure according to the following criteria:

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [5] [6] [7];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [8]; and
- SCCS scheme publications [9] [10] [11]

1.2 Recognition Agreements

The international arrangement on the mutual recognition of certificates based on the Common Criteria Recognition Arrangement had been ratified on 2 July 2014. The arrangement covers certificates with claims of compliance against collaborative protection profiles (cPPs) or evaluation assurance levels (EALs) 1 through 2 and ALC_FLR. Hence, the certification for this TOE is fully covered by the CCRA.

The Common Criteria Recognition Arrangement mark printed on the certificate indicates that this certification is recognised under the terms of this agreement by all signatory nations listed on the CC web portal (https://www.commoncriteriaportal.org).

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **11 August 2026**[1].

In cases of changes to the certified version of the TOE, the validity may be extended to new versions and releases provided the TOE sponsor applies for Assurance Continuity (i.e. re-certification or maintenance) of the revised TOE, in accordance with the requirements of the Singapore Common Criteria Scheme (SCCS).

The owner of the Certificate is obliged:

- When advertising the Certificate or the fact of the product's certification, to refer to and provide the Certification Report, the Security Target and user guidance documentation herein to any customer of the product for the application and usage of the certified product;
- To inform the SCCS immediately about vulnerabilities of the product that have been identified by the developer or any third party; and
- To inform the SCCS immediately in the case that relevant security changes in the evaluated life cycle has occurred or the confidentiality of documentation and information related to the TOE or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is no longer valid.

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [11]. Potential users should check the SCCS website (www.csa.gov.sg/programmes/csa-cc-product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: Securaze Eraser Engine version 2.0. The following table identifies the TOE deliverables.

Identifier	Version
Securaze-Engine	2.0

Table 4 - TOE Deliverable

The guide for receipt and acceptance of the above-mentioned TOE are described in the set of guidance documents.

Name and version	Version
Manual [1]	1.0.0
Work [2]	2.3.0
Mobile [3]	2.0.0

Table 5 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	Securaze-Engine v2.0
Security Target	“Security Target for the Eraser Engine, Securaze-Engine, Version 2.0” Version 4.0
Developer	Securaze AG
Sponsor	Securaze AG
Evaluation Facility	An Security Pte Ltd
Completion Date of Evaluation	10 August 2021
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_20006
Certificate Validity	5 years from date of issuance

Table 6: Additional Identification Information

4 Security Policy

The TOE's Security Policy is expressed by the set of Security Functional Requirements listed and implemented by the TOE.

The TOE implements policies pertaining to security functional classes "User Data Protection" and "Security Audit".

Specific details concerning the above-mentioned security policy can be found in Chapter 6 of the Security Target [4].

5 Assumptions & Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [4] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Environmental Assumptions	Description
OE.Time	The IT environment must provide a reliable time stamp and ensure that the time is correctly set.
OE.Platform	The underlying hardware, firmware and the operating system functions needed by the TOE shall work correctly, are not compromised by any malicious software and have no undocumented security critical side effects on the functions of the TOE.
OE.SpreadRetention	The operational environment provides a policy for data protection, which defines which places are allowed to store which data. Especially the used storage media are stipulated.
OE.Users	Users of the TOE are not careless, willfully negligent, or hostile and will follow the instructions in the guidance documentation.
OE.Admin	Administrators are not careless, willfully negligent, or hostile and will follow the instructions in the guidance documentation and the TOE will provide the necessary functions to support administrators in their management of the security of the TOE.
OE.Physical	The TOE is located in a restricted environment that provides protection from unmanaged access to the physical components and data interfaces of the TOE

Table 7: Environmental Assumptions

Details can be found in section 4.2 of the Security Target [4].

5.2 Clarification of Scope

The scope of evaluation is limited to the claims made in the Security Target [4].

5.3 Evaluated Configuration

The evaluated configuration in the Security Target [4] is as shown in Figure 3: TOE Evaluated Configuration (TOE within Securaze Work) and Figure 4 - TOE Evaluated Configuration (TOE within Securaze Mobile).

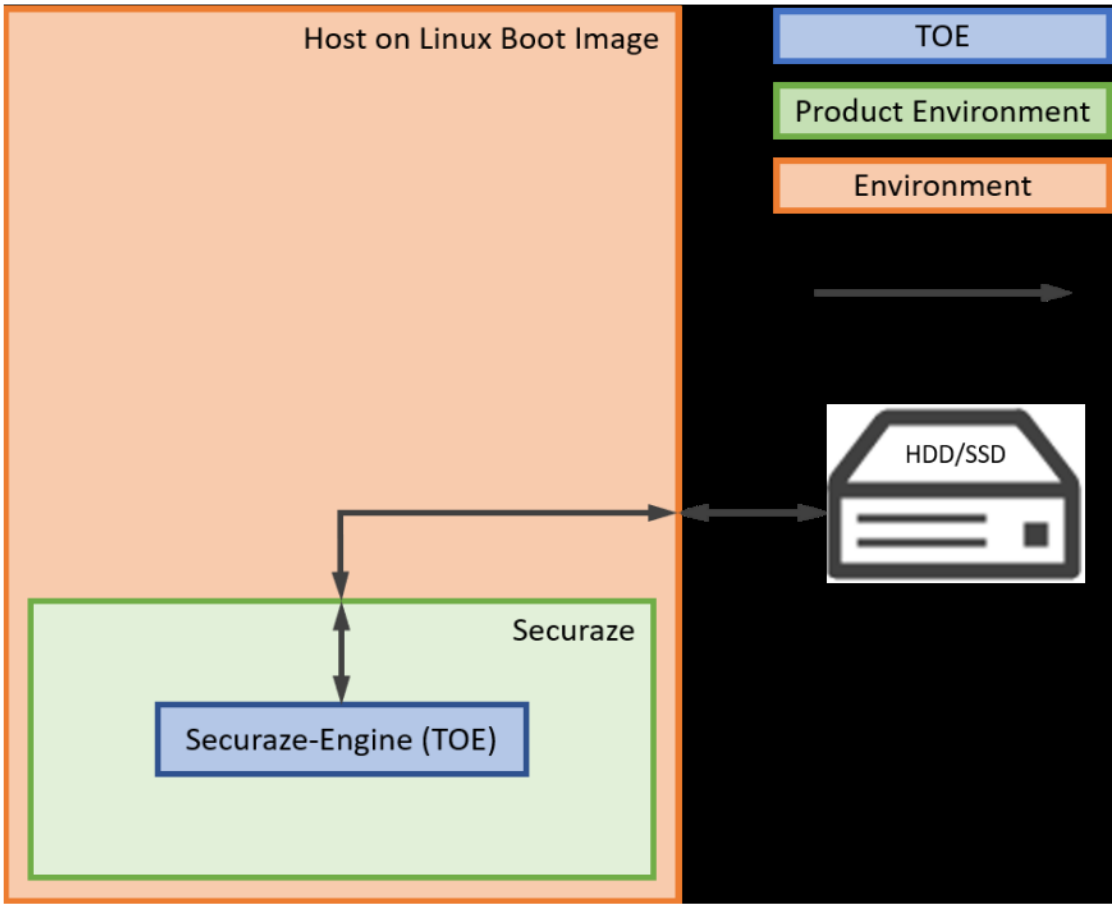

Figure 3: TOE Evaluated Configuration (TOE within Securaze Work)

To use Securaze Work, the user shall start a bootable Linux image (e.g., from a USB-Stick) including the Securaze Software Suite. The user then connect drives to the system and wipe these drives using Securaze Work that will trigger the Securaze-Engine (TOE) to perform the erasure process.

The Securaze-Engine (TOE) as part of the Securaze Work application is only responsible for the performance of the erasure, audit generation and verification of the successful eraser process.

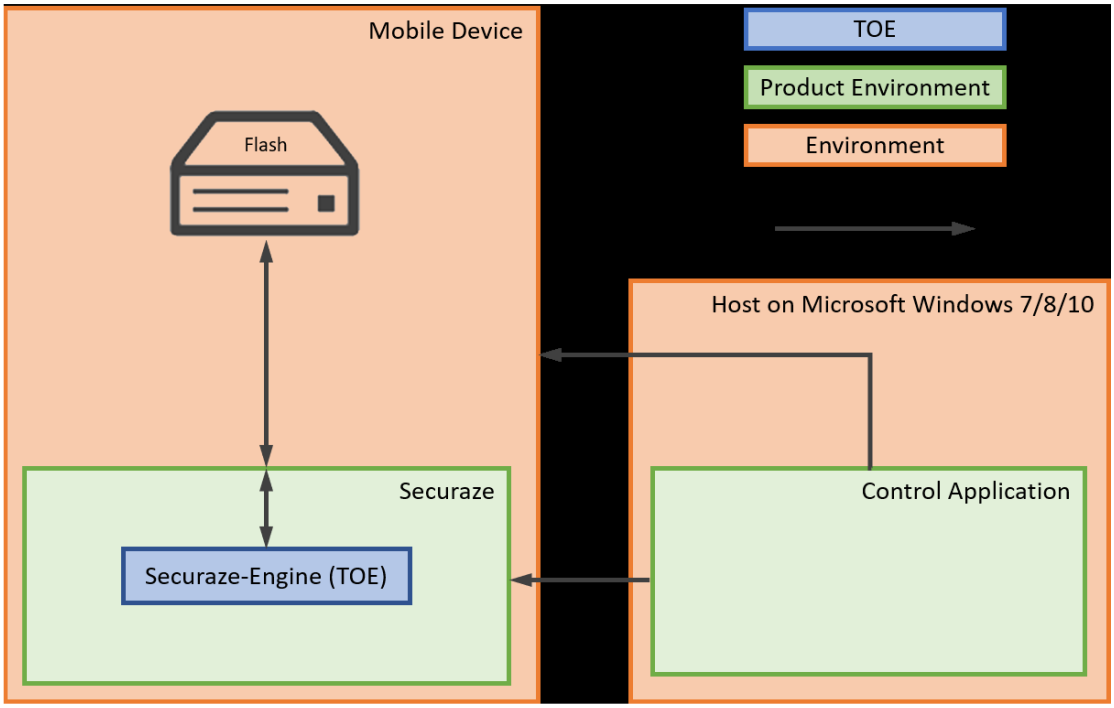

Figure 4 - TOE Evaluated Configuration (TOE within Securaze Mobile)

To use Securaze Mobile, the user shall connect the mobile device to the Windows PC running Securaze Control Application to upload the Securaze Mobile application to the phone. The Securaze Control Application then trigger the Securaze Mobile to initiate the factory reset (erasure) of the mobile device. Upon successful erasure, the Securaze Control Application will proceed to flash the original OS back to the mobile device.

The Securaze-Engine (TOE) as part of the Securaze Mobile application is only responsible for the performance of the erasure, audit generation and verification of the successful eraser process.

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities.

5.5 Non-TOE Components

The TOE requires additional components (i.e. hardware/software/firmware) for its operation. These non-TOE components include:

	Securaze WORK	Securaze MOBILE	Securaze DASHBOARD
Operating System (Host)	Securaze Linux Debian based custom linux distribution (Included in the Boot image)	Windows 10	Ubuntu 20.04 LTS Server
Operating System (Device)	n/a	Android >= 4.0 iOS >= 6	n/a
Web UI	Securaze Dashboard	Securaze Dashboard	n/a
Additional Software	-	-	-
Hardware Requirements	CPU: - RAM: 256 MB HDD Space: 0	CPU: 1 Ghz RAM: 1 GB HDD Space: 200mb	CPU: 64Bit Quad-Core RAM: 16 GB SSD Space: 256 GB
List of devices supported under this evaluation	**SSD**: Micron RealSSD C400 MTFDDAK128MAM-1J1 ADATA SU800 Kingston A400 SK.Hynix M2. SATA Kingston M2.NVME Samsung SAS Enterprise Flash – 520bps format **HDD**: Western Digital WD Blue 500GB (WD5000AAKX) Seagate Desktop HDD 500 GB (ST500DM002) HGST Travelstar 2.5-Inch 320GB (HTS725032A7E630) Seagate 3,5“ SATA Magnetic Seagate SAS Enterprise Magnetic – 520bps format	Mobile devices from • Android 4.0 • iOS 6	n/a

Table 8 -Required non-TOE Hardware/Software/Firmware

More information is available in section 1.4.2 of the Security Target [4].

6 Documentation

The evaluated documentation as listed in Table 5 - Guidance Document is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

7 IT Product Testing

7.1 Developer Testing (ATE_FUN)

7.1.1 Test Approach and Depth

The developer's tests cover all operational functions as described in the ST.

7.1.2 Test Configuration

Different brands of HDD, SSD, mobile phones (as described in section 1.4.2 in the ST) and the various erasure methods provided by the TOE were tested. The test for FPT_FLS.1 requires a customized the TOE to simulate errors when checking for the write patterns for verification of erasure.

7.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the ST. All test results from tested environments showed that the expected test results are identical to the actual test results.

7.2 Evaluator Testing (ATE_IND)

7.2.1 Test Approach and Depth

In accordance with the evaluated configuration, attackers are deemed to not have physical access to the TOE. Thus, the focus on the testing was placed on the TOE's erasure functionality. The evaluator sampled and repeated the developer's test cases that are relevant to the TOE's erasure functionality.

In addition, the evaluators also devised a set of independent tests that supplements or augments developer's existing test plan to gain assurance of the security of the TOE.

7.2.2 Test Configuration

A detailed test description was provided in the ATE document. Prior to running tests, the evaluator performed identification of the test environment and verification of the TOE.

7.2.3 Test Results

The developer's test reproduced were verified by the evaluator to conform to the expected results from the test plan.

7.3 Penetration Testing (AVA_VAN)

7.3.1 Test Approach and Depth

The approach chosen by the evaluator is commensurate with the assurance component chosen (AVA_VAN) treating the resistance of the TOE to an attack with the Basic attack potential. i.e. amongst other that the evaluator used sources of information publicly available to identify potential vulnerabilities in the TOE. The evaluator analysed which potential vulnerabilities are not applicable to the TOE in its operational environment

For the potential vulnerabilities being applicable to the TOE in its operational environment and, hence, which were candidates for testing applicable to the TOE in its operational environment, the evaluator devised the attack scenarios where these potential vulnerabilities could be exploited. For each such attack scenario he firstly performed a theoretical analysis on the related attack potential. Where the attack potential was Basic or near to Basic, the evaluator conducted penetration tests for such attack scenarios. He analysed then the results of these tests with the aim to determine, whether at least one of the attack scenarios with the attack potential Basic was successful.

The approach chosen by the evaluator is appropriate for the assurance component chosen (AVA_VAN.2), treating the resistance of the TOE to an attack with **Basic** potential.

The evaluator found no exploitable vulnerability in the TOE when operated in the evaluated configuration. No residual risks were identified.

8 Results of the Evaluation

The Evaluation Technical Report (ETR) was provided by the CCTL in accordance with the CC, CEM and requirements of the SCCS. As a result of the evaluation, the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 augmented by ALC_FLR.2 assurance package

This implies that the TOE satisfies the security requirements specified in the Security Target [4].

9 Obligations & Recommendations for Usage of the TOE

The documents as outlined in Table *5* - Guidance Document contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [4] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

Potential user of the product shall consider the results of the certification within his/her system risk management process. As attack methods and techniques evolve over time, he/she should define the period of time whereby a re-assessment of the TOE is required and convey such request to the sponsor of the certificate.

No additional recommendation was provided by the evaluators.

10 Acronyms

CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CCTL	Common Criteria Test Laboratory
CSA	Cyber Security Agency of Singapore
CEM	Common Methodology for Information Technology Security Evaluation
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
IT	Information Technology
PP	Protection Profile
SAR	Security Assurance Requirement
SCCS	Singapore Common Criteria Scheme
SFR	Security Functional Requirement
TOE	Target of Evaluation
TSF	TOE Security Functionality

11 Bibliography

[1] Securaze AG, “Manual, Version 1.0.0,” 2021.

[2] Securaze AG, “Work, Version 2.3.0,” 2021.

[3] Securaze AG, “Mobile, Version 2.0.0,” 2021.

[4] Securaze AG, “"Security Target for the Eraser Engine, Securaze-Engine, Version 2.0", Version 4.0, 3 August 2021”.

[5] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 1: Introduction and general model [Document Number CCMB-2017-04-001]. Version 3.1 Revision 5,” 2017.

[6] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 2: Security functional components [Document Number CCMB-2017-04-002], Version 3.1 Revision 5,” 2017.

[7] Common Criteria Maintenance Board (CCMB), “Common Criteria for Information Technology Security Evaluation - Part 3: Security assurance components [Document Number CCMB-2018-04-003] Version 3.1 Revision 5,” 2017.

[8] Common Criteria Maintenance Board (CCMB), “Common Methodology for Information Technology Security Evaluation - Evaluation Methodology [Document Number CCMB-2017-04-004], Version 3.1 Revision 5,” 2017.

[9] Cyber Security Agency of Singapore (CSA), “SCCS Publication 1 - Overview of SCCS, Version 5.0,” 2018.

[10] Cyber Security Agency of Singapore (CSA), “SCCS Publication 2 - Requirements for CCTL, Version 5.0,” 2018.

[11] Cyber Security Agency of Singapore (CSA), “SCCS Publication 3 - Evaluation and Certification, Version 5.0,” 2018.

[12] An Security, “Evaluation Technical Report EAL 2 CC Evaluation of Securaze-Engine, Version 1.0, 10 August 2021”.

----------End of Report ----------