SECURAZE

# Security Target for the Eraser Engine „Securaze-Engine“, Version 2.0

| | |
|---|---|
| Autor: | Securaze AG |
| Version: | 4.0. |
| Datum: | 03.08.2021 |

Company Address

Securaze AG,
Schutzengelstraße 36
6340 Baar
Switzerland

This page has been intentionally left blank.

**Contents**

Page

**1 ST INTRODUCTION ... 5**
1.1 ST Reference ... 5
1.2 TOE Reference ... 5
1.3 Specific Terms ... 5
1.4 TOE Overview ... 5
1.4.1 TOE Type ... 6
1.4.2 Required non-TOE hardware/software/firmware ... 6
1.5 TOE Description ... 8
1.5.1 General description ... 8
1.5.2 Securaze WORK (erasure of HDD/SSD) ... 8
1.5.3 Securaze MOBILE (erasure Mobile Devices) ... 11
1.5.4 TOE Deliverables ... 13
1.5.5 TOE Boundaries ... 13
**2 CONFORMANCE CLAIMS ... 15**
2.1 CC Conformance Claims ... 15
2.2 PP Claim ... 15
2.3 Package Claim ... 15
**3 SECURITY PROBLEM DEFINITION ... 16**
3.1 Assets ... 16
3.2 Subjects ... 16
3.3 Objects ... 16
3.4 Assumptions ... 16
3.5 Threats ... 17
3.6 Organizational Security Policies (OSPs) ... 17
**4 SECURITY OBJECTIVES ... 18**
4.1 Security Objectives for the TOE ... 18
4.2 Security Objectives for the Environment ... 18
4.3 Security Objectives Rationale ... 19
4.3.1 Countering the threats ... 19
4.3.2 Covering the assumptions ... 19
4.3.3 Covering the OSPs ... 20
**5 EXTENDED COMPONENT DEFINITION ... 21**
5.1 Definition of requirement ... 21
5.2 FDP_RIP.3 Residual Information Protection by specific destruction method ... 21
**6 SECURITY REQUIREMENTS ... 22**
6.1 Security Functional Requirements ... 22
6.2 Class FDP: User Data Protection ... 22
6.2.1 FDP_RIP.3 Residual Information Protection by specific deallocation method . 22
6.3 Class FAU: Security Audit ... 22
6.3.1 FAU_GEN.1: Audit Data Generation ... 22
6.4 Class FPT: Protection of the TSF ... 23
6.4.1 FPT_FLS.1 Failure with preservation of secure state ... 23
6.5 Security Assurance Requirements ... 23
6.6 Security Requirements Rationale ... 24
6.6.1 Rationale for the Security Functional Requirements (SFRs) ... 24
6.7 Rationale for the Security Assurance Requirements (SARs) ... 25
6.7.1 Fulfilment of the Dependencies ... 25

**7 TOE SUMMARY SPECIFICATION ..... 26**
7.1 SF Erasure Process ..... 26
7.2 SF Audit ..... 26
**8 REFERENCES ..... 27**

# 1 ST Introduction

## 1.1 ST Reference

| | |
|---|---|
| Document Title: | Security Target for the Eraser Engine „Securaze-Engine“, Version 2.0 |
| Document Version: | 4.0 |
| Document Date: | 2021-08-03 |

## 1.2 TOE Reference

| | |
|---|---|
| TOE Name: | Securaze-Engine |
| TOE Version: | 2.0 |
| Developer: | Securaze AG |
| Product Type: | Eraser Engine for Secure Erasure of HDD/SSD and Flash Memory |

## 1.3 Specific Terms

**Table 1 – Terms**

| Term | Description |
|---|---|
| DCO | Device Configuration Overlay |
| Erasure Method | Properties: Pattern, Repetition (e.g. DoD, BSI, Securaze SSD): |
| FTL | Flash Translation Layer |
| HDD | Hard Disk Drive |
| HPA | Hidden Protected Area |
| SSD | Solid State Disk |
| Storage Device | Mass storage device. Examples: HDD, SSD, SSHD, USB-Flash-memory |

## 1.4 TOE Overview

The Target of Evaluation (TOE) is the eraser engine of Securaze.

Securaze Software Suite is a software tool for secure erasure of HDD, SDD and memory of mobile phones. The eraser software is a part of the complete Lifecycle: There is the software to erase HDD/SSD – Securaze Work, the software to erase Mobile Devices – Securaze Mobile and a web user interface – Securaze Dashboard.

Dashboard:

Securaze Dashboard is a web user interface, where the .ISO file to install Securaze Work or Securaze Mobile can be downloaded.

In Securaze Dashboard, settings are made for the use of Securaze Work and Securaze Mobile: the user can create user-profiles to login to Securaze Work or Securaze Mobile, make settings for the management of the assets and download the erasure reports.
Securaze Suite consists of different Securaze Clients dedicated for different usages:

Securaze Work (Erasure of HDD/SSD):

In this version the user can start a bootable Linux image (e.g., from a USB-Stick) including Securaze Work to wipe the connected drives in a secure way. Securaze-Engine (TOE) as part of the complete Securaze product is responsible for performing the secure eraser process.

Securaze MOBILE (erasure of Mobile Devices):

In this version, Securaze Mobile software is installed on a Windows PC to which the mobile phone is connected to initiate a factory reset on the mobile phone and upload the Securaze Application to the phone. Securaze-Engine (TOE) as part of this application is then responsible for performing the secure eraser process.

Both versions contain the same Securaze-Engine which is responsible for performing the secure eraser process, audit generation and verification of the successful eraser process. The TOE as well as the complete product are designed to fulfil the need for protection of sensitive data stored on drives and mobile phones before these get recycled or destroyed. Please be aware that the TOE only consists of the Securaze-Engine. Securaze Suite itself is not part of the TOE but necessary environment.

### 1.4.1 TOE Type

Securaze-Engine is the secure eraser engine of Securaze responsible to erase HDD/SSD/Mobile Devices in a secure and permanently way.

### 1.4.2 Required non-TOE hardware/software/firmware

**Table 2 – Required non-TOE hardware/software/firmware**

| | **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<br>iOS >= 6 | n/a |
| Web UI | Securaze Dashboard | Securaze Dashboard | n/a |
| Additional Software | - | - | - |
| Hardware Requirements | CPU: -<br>RAM: 256 MB<br>HDD Space: 0 | CPU: 1 Ghz<br>RAM: 1 GB<br>HDD Space: 200mb | CPU: 64Bit Quad-Core<br>RAM: 16 GB<br>SSD Space: 256 GB |
| List of devices supported under this evaluation | SSD:<br>Micron RealSSD C400 MTFDDAK128MAM-1J1<br>ADATA SU800 | Mobile devices from<br>• Android 4.0<br>• iOS 6 | n/a |

| | **Securaze WORK** | **Securaze MOBILE** | **Securaze Dashboard** |
|---|---|---|---|
| | Kingston A400<br>SK.Hynix M2. SATA<br>Kingston M2.NVME<br>Samsung SAS Enterprise Flash – 520bps format<br>HDD:<br>Western Digital WD Blue 500GB (WD5000AAKX)<br>Seagate Desktop HDD 500 GB (ST500DM002)<br>HGST Travelstar 2.5-Inch 320GB (HTS725032A7E630)<br>Seagate 3,5“ SATA Magnetic<br>Seagate SAS Enterprise Magnetic – 520bps format | | |

Application Note: Technical identical devices (compared to the supported devices listed) and other compatible devices can also be wiped with the Securaze-Engine.

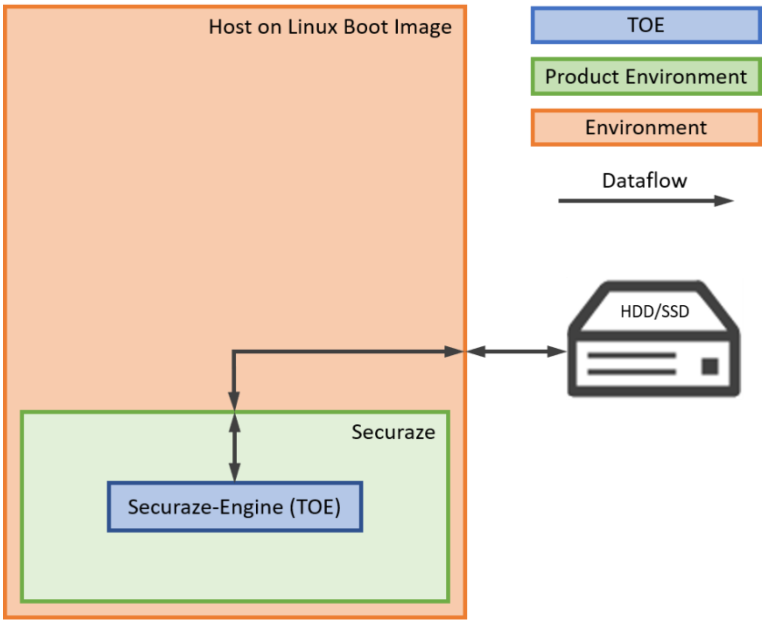
## 1.5 TOE Description

### 1.5.1 General description

As described in the TOE Overview the TOE is the engine of the product Securaze. Independently from the product version (e.g., Securaze Work or Securaze Mobile) the engine is always the same. To introduce the different versions of Securaze and to give a more detailed understanding of the functioning of the engine both versions are described in a more technically way in the following chapters.

### 1.5.2 Securaze WORK (erasure of HDD/SSD)

**Figure 1.1 – Overview Securaze WORK**



To use Securaze Work, the user can start a bootable Linux image (e.g., from a USB-Stick). The user can then connect drives to this system and wipe these drives in a secure way. Securaze-Engine (TOE) as part of the complete Securaze Work application is responsible for performing the secure eraser process.

As can be seen in **Figure 1.1,** there are four parts of the complete product that will be described in the following subchapters as they are all necessary for the correct operation of the TOE . In general , it can be subdivided into the TOE, the Product Environment (in which the TOE is embedded ) and the general environment performing general services to support the product environment and the TOE (e.g. Linux operating system). Nevertheless, even if all of these parts are necessary for the correct operation please keep in mind that only Securaze -Engine (among the guidance documentation ) is the TOE. All other parts are part of the environment.

### 1.5.2.1 NON-TOE components

**Host on Linux Boot Image**

The host is running on Securaze Linux (a custom Securaze Debian based linux distribution) and is provided as an image. This image normally is located on a USB device from which the computer can boot. This operating system generally is used to provide the computer with the basic functionality of an operating system and to provide the necessary runtime environment for the Securaze Work (including the Securaze-Engine (TOE)).

**Securaze**

The Securaze Dashboard enables the user to map the complete end-of-life process of IT devices (assets). The Securaze Dashboard offers:

- Erasure of HDDs
- Erasure of SSDs
- Downloadable erasure reports
- Verification of erasure
  Uniform look & feel across all modules

Furthermore , the SECURAZE -Engine (TOE) is embedded into the Securaze Work and gives the user the possibility to use and control the TOE by a user-friendly graphical user interface . Securaze Work application is generated by the Dashboard (as an Securaze Linux image).

**HDD/SSD/Flash Memory**

In order to enable the TOE to securely erase data stored on a memory device special requirement need to be fulfilled by this device . In case a user tries to erase non-supported device , the software will stop the operation and give a corresponding warning . Thereby it is ensured that the user always knows if a secure erasure is possible for the connected device or not.

The following devices including the specified memory chips are a selection of supported devices for secure erase by the TOE. Technical identical devices (compared to the supported devices listed) and other compatible devices can also be wiped with the Securaze-Engine. A list of erased storages from different vendors and models can be found in the Securaze Work Manual in chapter System Requirements.

| **Type** | **Device** | **Memory Chips/Controller** |
|---|---|---|
| SSD | Micron RealSSD C400 MTFDDAK128MAM-1J1 | Marvell 88SS9174-BLD2 |
| SSD | ADATA SU800 | Silicon Motion |
| SSD | Kingston A400 | Phison |
| SSD | SK.Hynix M2. SATA | N/A |
| SSD | Kingston M2.NVME | N/A |
| SSD | Samsung SAS Enterprise Flash – 520bps format | N/A |
| SSD | NoName 2,5“ Flash | N/A |

| Type | Device | Memory Chips/Controller |
|---|---|---|
| HDD | Western Digital WD Blue 500GB (WD5000AAKX) | N/A |
| HDD | Seagate Desktop HDD 500 GB (ST500DM002) | N/A |
| HDD | HGST Travelstar 2.5-Inch 320GB (HTS725032A7E630) | N/A |
| HDD | Seagate 3,5“ SATA Magnetic | N/A |
| HDD | Seagate SAS Enterprise Magnetic – 520bps format | N/A |

**Table 3: Selection of supported Devices**

### 1.5.2.2 TOE components

**Securaze-Engine**

The Securaze engine provides methods for erasing different types of devices. The general Workflow is uniform for all erasure-devices, the specific erasure functionality is specifically implemented per device type as the different devices offer different commands and techniques for erasure. For this reason, the secure erasure can only be done on supported devices as listed in Table 3.

Erasure:

For the erasure process it needs to be differed to the kind of device.

For classical HDDs the erasure functionality uses the DoD 5220.22-M, DoD 5220.22-M Standard, 5220.22-M ECE, NIST800-88 Purge, NIST800-88 Clear or Infosec Standard 5 erasure standard for overwriting HDDs.

For SSDs the erasure functionality uses a self-developed algorithm (SEC-2018-SSD FM) to perform the erasure. Thereby the Securaze erasure method ensures for SSDs that every single flash storage cell gets sufficiently overwritten by bypassing the Flash Translation Layer.

Difference between HDD and SSD erasure

The main difference between the erasure of HDDs and SSDs is that HDDs may just be overwritten with standard erasure methods like DoD 5220.22-M, DoD 5220.22-M Standard, 5220.22-M ECE, NIST800-88 Purge, NIST800-88 Clear or Infosec Standard 5. The reason is that HDDs don’t optimize the write to the storage. So, every write call will just plain be written into the storage. The same method can’t be used for SSDs because the FTL (Flash Translation Layer) tries to optimize the longevity of the NAND memory cells by relocate each write process to another memory cell. Furthermore, the FTL tries to compress same written data and logically disables cells which are not good enough for regular usage.

Because of this standard HDD erasure methods are failing and reduce the durability of the NAND memory cells.

Logging:

The erasure results are collected for each device type individually. The results are used by Securaze Dashboard to generate downloadable erasure reports.

Verification:

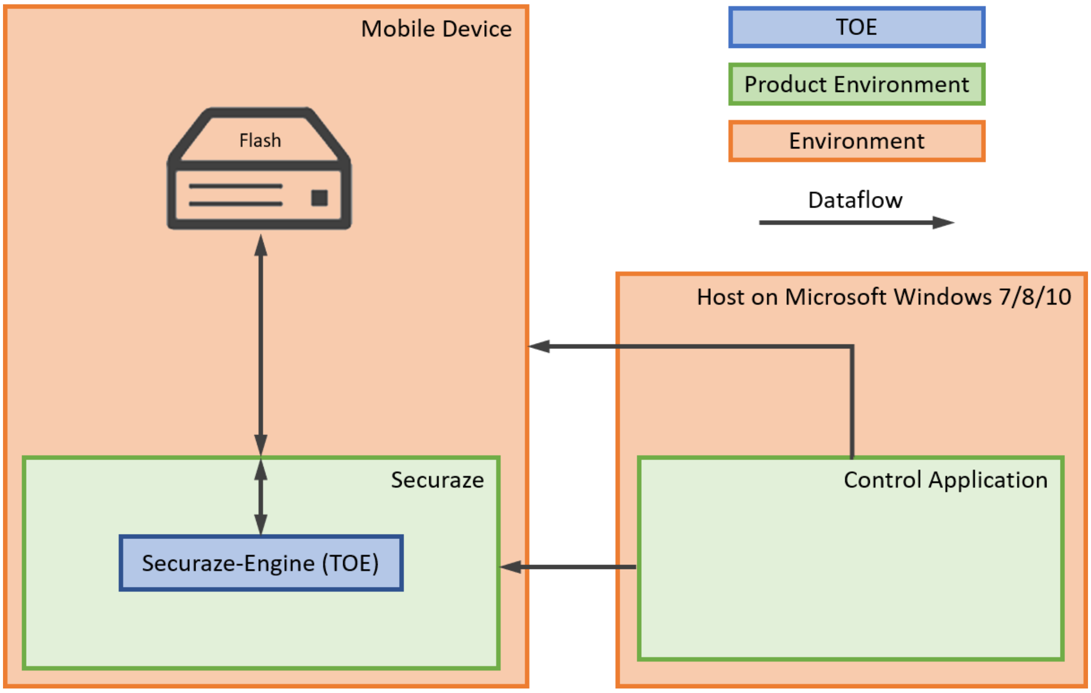
The erasure results can be optionally verified after the erasure. The verification method depends on the erasure method.

To verify the results for HDDs the verification of erasure can either be done after each pass of DoD 5220.22-M, after the last pass or skipped.

To verify the results for SSDs the verification of erasure searches for specific patterns written on the flash memory.

### 1.5.3 Securaze MOBILE (erasure Mobile Devices)

**Figure 1.2 – Overview Securaze MOBILE**



To use Securaze Mobile, the user shall connect the mobile device to the Windows PC running Securaze Mobile desktop application to upload the Securaze Mobile application to the mobile device. Securaze -Engine (TOE) as part of the complete Securaze Mobile application is responsible for performing the secure eraser process.

As can be seen in **Figure 1.2,** there are six parts of the complete product that will be described in the following subchapters as they are all necessary for the correct operation of the Securaze - Engine. In general, it can be subdivided into the TOE, the Product Environment (in which the TOE is embedded) and the general environment performing general services to support the product environment and the TOE (e.g. Windows or the mobile operating system). Nevertheless, even if all of these parts are necessary for the correct operation please keep in mind that only Securaze -Engine (among the guidance documentation) is the TOE. All other parts are part of the environment.

#### 1.5.3.1 NON-TOE components

**Host on Microsoft Windows**

The host is running on Microsoft Windows. The operating system generally is used to provide the computer with the basic functionality of an operating system and to provide the necessary runtime environment for the Securaze Mobile Desktop Application (Control Application).

**Control Application**

The Securaze Mobile Desktop Application (Control Application) controls the Workflow during the erasure process. The main functions are:

- Controlling the mobile devices which requires activated USB Debug Mode
- Starting factory reset of the mobile device
    - Updating firmware of the mobile device if available
- Installs Securaze Mobile App (including the Securaze-Engine) on the mobile device.

**Mobile Device**

The Securaze Engine for Mobile Devices supports the mobile devices listed in Chapter 1.4.3.

**Flash Memory**

On mobile devices there is NAND flash installed, similar to SSDs. In difference to SSDs the mobile devices are far easier implemented:

- No DCO: No spare memory for defect memory cells
- No HPA: No secret / invisible storage
- No FTL: No logic to improve durability of the flash cells available

Please be aware that only the in section 1.4.3. mentioned NAND flashes are supported.

**Securaze**

The Securaze Dashboard enables our customers to map the complete end-of-life process of IT devices (assets). The Securaze Dashboard offers:

- Erasure of Mobile Devices,
- Downloadable erasure reports,
- Verification of erasure, and
- Uniform look & feel across all modules

Furthermore, the SECURAZE-Engine (TOE) is embedded into the Securaze Mobile application and user can use and control the TOE by a graphical user interface.

#### 1.5.3.2 TOE components

**Securaze-Engine**

The Securaze engine provides methods for erasing different types of mobile devices.

Erasure:

The erasure functionality uses the self-developed SSD erasure method SEC-2018-SSD FM for overwriting Flash Memory of Mobile Devices.

For the Android Advanced Erasure, a combination of methods is used to reach storage areas which are unavailable from regular Android operating system.

To enable access to this storage areas a vendor specific firmware is installed on the device. This firmware allows to install the native Securaze Android Advanced Erasure tool on the system. This tool contains the Securaze erasure engine and uses the self-developed SEC-

2018-SSD FM algorithm to erase the storage of the device in a low-level way comparable to regular SSD erasure.

Logging:

The erasure results are collected for each device type individually. The results used by the Securaze Dashboard to generate downloadable erasure reports.

Verification:

The erasure results can be optionally verified after the erasure. The verification method depends on the erasure method.

To verify the results for Mobile Devices the verification of erasure happens after the erasure of the storage.

To verify the results for Android Advanced Erasure the verification of erasure searches for specific patterns written on the flash memory.

## 1.5.4 TOE Deliverables

| Category | Description | Version | Remarks |
|---|---|---|---|
| Software | Securaze-Engine | 2.0 | The engine is embedded in the software suite.<br>It will be delivered by Securaze personnel and installed |
| Guidance Documents | Manual - Local hosted Securaze Dashboard | 1.0.0 | Delivered as PDF (CD) or via download link provided by Securaze |
| | Work | 2.3.0 | |
| | Mobile | 2.0.0 | |

Securaze software is available to download on Securaze Dashboard. A description which file you need to download can be found in Securaze Manual.

Securaze Dashboard is delivered via Securaze authorized personnel.

## 1.5.5 TOE Boundaries

### 1.5.5.1 Physical Boundary

As only one module of Securaze namely the Securaze-Engine is the Target of Evaluation the physical scope can be seen as a binary file which is imported by the product environment. The binary itself is included in downloadable Linux image (Securaze WORK) or in the installer of Securaze (Securaze MOBILE).

The guidance documentation are delivered via CD or via download link on Securaze portal.

### 1.5.5.2 Logical Boundary

When the product environment (Securaze) is started it uses the Securaze-Engine which is a binary including the security features:

1. Secure Erasure of HDD/SDD/Mobile Android and iOS Devices:

- Overwriting HDD according to DoD 5220.22-M Standard which means
    - Pass 1: Overwrite all addressable locations with binary zeroes.
    - Pass 2: Overwrite all addressable locations with binary ones (the compliment of the above).
    - Pass 3: Overwrite all addressable locations with a random bit pattern
    - Verify the final overwrite pass.
- Overwriting HDD according to DoD 5220.22-M ECE
- Overwriting HDD according to NIST800-88 Purge
- Overwriting HDD according to NIST800-88 Clear
- Overwriting HDD according to HMG Infosec Standard 5
- Overwriting SSD/Mobile Devices with a self-developed method SEC-201SSD FM

2. Audit Generation:

- Logging of all security relevant events
- Logging of success/failure during eraser process
- Logging of used configuration parameters

3. Verification of the successful eraser process

- Verify by chosen erasure method overwritten locations
- Verify the SSD/Flash overwritten locations by search for a known pattern

# 2 Conformance Claims

## 2.1 CC Conformance Claims

The Security target and the TOE claim conformance to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017, CCMB-2017-04-001,
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-002,
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, Version 3.1, Revision 5, April 2017, CCMB-2017-04-003.

The TOE is CC Part 2 [CC2] extended and CC Part 3 [CC3] conformant.

## 2.2 PP Claim

The Security Target does not claim conformance to a Protection Profile.

## 2.3 Package Claim

The Security Target claims to be conformant to the Assurance Packet EAL2 augmented with ALC_FLR.2.

# 3 Security Problem Definition

## 3.1 Assets

The main purpose of Securaze-Engine is to ensure the secure erasurege devices. All assets to be protected by the TOE are listed in the table below:

**Table 4 – Assets**

| Assets | Description |
|---|---|
| User data | Data for the TOE users that does not affect the operation of the TSF. It contains data stored on the device which shall be erased by the TOE. Such data can be for example:<br>• Pictures<br>• Videos<br>• Text files<br>• Mails<br>• Etc. |

## 3.2 Subjects

The following table lists all subjects that interact with the TOE.

**Table 5 – Subjects**

| Subject | Description |
|---|---|
| User | A person that executes Securaze including Securaze-Engine to delete storage devices in a way that they cannot be recovered. |

## 3.3 Objects

The following table lists all subjects that interact with the TOE.

**Table 6 – Objects**

| Object | Description |
|---|---|
| Device | Device which shall be securely erased. |

## 3.4 Assumptions

**Table 7 – Assumptions**

| Assumptions | Description |
|---|---|
| A.Time | The underlying platform provides a reliable time stamp to support the security functions of the TOE |
| A.Platform | The underlying hardware, firmware and the operating system functions needed by the TOE are working correctly, are not |

| Assumptions | Description |
|---|---|
| | compromised by any malicious software, and have no undocumented security critical side effects on the functions of the TOE. |
| A.Users | Users of the TOE are not careless, willfully negligent, or hostile and will follow the instructions in the guidance documentation. |
| A.Admin | The TOE will provide the necessary functions to support administrators in their management of the security of the TOE. Administrators are not careless, willfully negligent, or hostile and will follow the instructions in the guidance documentation. |
| A.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 |

## 3.5 Threats

**Table 8 – Threats**

| Threats | Description |
|---|---|
| T.DataRecovery | An attacker getting access to a storage device erased by the TOE is able to compromise the confidentiality of the original data that was stored on it, by recovering these data. |

## 3.6 Organizational Security Policies (OSPs)

**Table 9 – OSPs**

| OSPs | Description |
|---|---|
| OSP.Audit | The TOE shall provide information of the erasure process, consisting of erasure success or failure, the date erasure was performed, the erasure standard used and information about the content that was erased. |
| OSP.SpreadRetention | In the policy for data protection, those responsible for the TOE must define which places are allowed to store which data. The goal for limitation principle, limitation of data processing to the extent necessary with regard to data avoidance, and limitation of storage has to be realised. Especially the used storage media and the storage location in the organisation has to be defined. |

# 4 Security Objectives

## 4.1 Security Objectives for the TOE

**Table 10 – Security Objectives**

| Security Objective for the TOE | Description |
|---|---|
| O.Erasure | The TOE is able to erase all data from the device selected by the user in such a way that restoring the original data will fail. |
| O.Audit | The TOE shall provide log data about the storage device erasure process which include information about success or failure, used erasure standard and the time of the erasure process. |

## 4.2 Security Objectives for the Environment

**Table 11 – Security Objectives for the Environment**

| Security Objective for the Environment | 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 |

## 4.3 Security Objectives Rationale

The following table provides a mapping of security objectives to threats, OSPs and assumptions. the following sections provide a more detailed explanation of this mapping.

| | T.DataRecovery | A.Time | A.Platform | A.Users | A.Admin | A.Physical | OSP.Audit | OSP.SpreadRetention |
|---|---|---|---|---|---|---|---|---|
| O.Erasure | X | | | | | | | |
| O.Audit | | | | | | | X | |
| OE.Time | | X | | | | | X | |
| OE.Platform | | | X | | | | | |
| OE.SpreadRetention | | | | | | | | X |
| OE.Users | | | | X | | | | |
| OE.Admin | | | | | X | | | |
| OE.Physical | | | | | | X | | |

**Table 12: Mapping of security objectives to threats, OSPs and assumptions**

### 4.3.1 Countering the threats

T.DataRecovery Security objective O.Erasure ensures that all data from the device selected by the user is erased in such a way that restoring the original data will fail.

### 4.3.2 Covering the assumptions

The following statements can directly be derived

| | |
|---|---|
| A.Time | is covered by the security objective OE.Time. |
| A.Platform | is covered by the security objective OE.Platform. |
| A.Users | is covered by the security objective OE.Users. |
| A.Admin | is covered by the security objective OE.Admin. |
| A.Physical | is covered by the security objective OE.Physical. |

### 4.3.3 Covering the OSPs

OSP.Audit Security Objective ensures that information about the erase process will be performed. OE.Time ensures that a time stamp is provided.

OSP.SpreadRetention OE.SpreadRetention ensures that all used storage media will be included in the erase process.

# 5 Extended Component Definition

This section specifies the extended SFRs for the TOE.

## 5.1 Definition of requirement

## 5.2 FDP_RIP.3 Residual Information Protection by specific destruction method

FDP_RIP.3 is analog to FDP_RIP.1 except, that it applies the deallocation of resources to the used destruction method.

**Component levelling:**

FDP__RIP Residual Information Protection
3

FDP_RIP.3 is not hierarchical to any other component within the FDP_RIP family.

**Management:**

See management description specified for FDP_RIP.1 in [CC2].

**Audit:**

See audit requirement specified for FDP_RIP.1 in [CC2].

| **FDP_RIP.3** | **Residual Information Protection by specific destruction method** |
|---|---|
| Hierarchical to: | No other component. |
| Dependencies: | No dependencies. |
| FDP_RIP.3.1 | The TSF shall ensure that any previous information content of a resource is made unavailable upon the [selection: *allocation of the resource to, deallocation of the resource from*] in accordance with a specified destruction method [assignment: *list of destruction method*] the following objects: [assignment: *list of objects*] |

# 6 Security Requirements

This chapter describes the Security Functional and the Assurance Requirements which have to be fulfilled by the TOE. Those requirements comprise functional components from [CC2] and the assurance components as defined for the EAL3 from [CC3].

The following notations are used:

- **Refinement** operations (denoted by **bold text**): is used to add details to a requirement, and thus further restricts a requirement. In case that a word has been deleted from the original text this refinement is indicated by ~~**crossed out bold**~~ text.
- **Selection** operation (denoted by underlined text): is used to select one or more options provided by the [CC] in stating a requirement.
- **Assignment** operations (denoted by *italicized text*): is used to assign a specific value to an unspecified parameter, such as the length of password.
- **Iteration** operation: are identified with a suffix in the name of the SFR.

## 6.1 Security Functional Requirements

## 6.2 Class FDP: User Data Protection

### 6.2.1 FDP_RIP.3 Residual Information Protection by specific deallocation method

Hierarchical to: No other components

Dependencies: No dependencies

FDP_RIP.3.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from in accordance with a specified destruction method

1. *Overwrite according to*
    - *DoD 5220.22M*
    - DoD 5220.22-M ECE
    - NIST800-88 Purge
    - NIST800-88 Clear or
    - HMG Infosec Standard 5
2. *Self-developed method: SEC-2018-SSD FM*

the following objects:

3. *HDD*
4. *SDD*
5. *Mobil*

## 6.3 Class FAU: Security Audit

### 6.3.1 FAU_GEN.1: Audit Data Generation

Hierarchical to: No other components

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1The 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 minimum level of audit; and
c) *erasure as described in FDP_RIP.3*.

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the ST, [
   - *the data erased*
   - *type of operation performed (administrator defined wipe pattern)*
   - *number of overwrites performed*
   - *process duration*
   - *date and time operation was completed*
   - *operation result*
   - *total number of disk sector read/write errors, if any*
   - *total uncleaned or unreadable disk sectors, if any*
   - *current user (user-defined name of person performing the wipe)*].

## 6.4 Class FPT: Protection of the TSF

### 6.4.1 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of

failures occur: Verification of secure erasure fails

.

## 6.5 Security Assurance Requirements

The following table summarizes the Security Assurance Requirements for EAL2 as defined in [CC3].

| Assurance Class | Assurance Component |
|---|---|
| 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** | **Assurance Component** |
|---|---|
| ADV: Development | ADV_ARC.1 Security architecture description |
| | ADV_FSP.3 Functional specification with complete summary |
| | ADV_TDS.2 Architectural design |
| AGD: Guidance documents | AGD_OPE.1 Operational user guidance |
| | ADG_PRE.1 Preparative procedures |
| ALC: Life-cycle support | ALC_CMC.3 Authorisation controls |
| | ALC_CMS.3 Implementation representation CM coverage |
| | ALC_DEL.1 Delivery procedures |
| | ALC_DVS.1 Identification of security measures |
| | ALC_LCD.1 Developer defined life-cycle model |
| | ALC_FLR.2 Flaw reporting procedures |
| ATE: Tests | ATE_COV.2 Analysis of coverage |
| | ATE_DPT.1 Testing: basic testing |
| | ATE_FUN.1 Functional testing |
| | ATE_IND.2 Independent testing – sample |
| AVA: Vulnerability assessment | AVA_VAN.2: Vulnerability analysis |

## 6.6 Security Requirements Rationale

### 6.6.1 Rationale for the Security Functional Requirements (SFRs)

#### 6.6.1.1 Fulfilment of the Security Objectives

The following table shows that the security functional requirements fulfill the Security Objectives for the TOE:

| **Security Objective for the TOE** | **Security Functional Requirement** | **Rationale** |
|---|---|---|
| O.SecureErasure | FDP_RIP.3<br>FPT_FLS.1 | The security objective is fulfilled by FDP_RIP.3 that ensures that the erasure of storage devices can be performed, by user. FPT_FLS.1 that ensures that a secure state is preserved when failed write occurs. |
| O.Audit | FAU_GEN.1 | The security objective is fulfilled by FAU_GEN.1 that ensures that the log data required are created by the TOE. |

**Table 13: Fulfilment of Security Objectives**

#### 6.6.1.2 Fulfilment of the Dependencies

The following table shows how each dependency of the security functional requirements is fulfilled:

| Security Functional Requirement | Dependency | Dependency fulfilled |
|---|---|---|
| FDP_RIP.3 | -- | -- |
| FAU_GEN.1 | FPT_STM.1 | The dependency is fulfilled by the environment. Cf. OE.Time. |
| FPT_FLS.1 | -- | -- |

**Table 14: Fulfilment of SFR Dependencies**

## 6.7 Rationale for the Security Assurance Requirements (SARs)

The assurance package EAL2 has been chosen because it “permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises. EAL2 is applicable in those circumstances where developers or users require a moderate level of independently assured security and require a thorough investigation of the TOE and its development without substantial re-engineering.” [CC3 §105f].

### 6.7.1 Fulfilment of the Dependencies

The dependencies of the assurance requirements taken from EAL2+ ALC_FLR.2 are fulfilled automatically.

# 7 TOE Summary Specification

The following Table gives an overview of the TOE security functions (SF) described in this section and their corresponding security functional requirements (SFR). Each SF is described separately in one of the following subchapters.

## 7.1 SF Erasure Process

The TOE erases existing data by overwriting it. The erasure process depends on the storage media. Overwriting operation consists in sequential steps of write and verify data values.

- The target device must be overwritten by an algorithm defined in FDP_RIP.3.

The following steps are carried out during the erasure procedure:

- Remove freeze lock for all devices
- Reset and Verify Host Protected Area (HPA)
- Reset and Verify Device Configuration Overlay (DCO)
- Reset and Verify Remapped Sectors
- Write and Verify verification-pattern on specific places of the device before and after each pass (FPT_FLS.1). If verification fails, erasure will stopped and the result will be logged.
- Remove file system
- Apply erasure method defined in FDP_RIP.3.

## 7.2 SF Audit

The Audit contains a secure erase audit and reporting.

**Securaze Erase Audit and Report**
The secure erase audit is the result of the erasure of each device. The secure erase audit is generated by the TOE (FAU_GEN.1) and will be relayed back to the Securaze Dashboard. It will be stored in the database. The reports are available for download in PDF format in Securaze Dashboard. These reports will be signed by an authenticated user.

# 8 References

[ONFI] Open NAND Flash Interface Specification, Revision 4.1, 12 12 2017, www.onfi.org