Common Criteria Security Target for YouWipe Erasure Tool 4 with WipeCenter 4

Document Version: 6.0

Date: 30.07.2020

1 Security Target Introduction

1.1 ST reference

1.1.1 ST Identification

Security Target Document for Youwipe version 4.0 with WipeCenter version 4.0.

1.1.2 ST version[1]

6.0

1.1.3 ST date

July 30, 2020

1.2 TOE reference

1.2.1 TOE identification

Youwipe Erasure Tool 4 with WipeCenter 4 report management application

1.2.2 TOE version

Youwipe Version 4.1.48[2], WipeCenter Version 4.0.43

1.2.3 User guidance version

This Security Target document refers to the following User Guidance documents:

Youwipe Erasure Tool User Manual, version 2.0.6

WipeCenter User Manual, version 2.0.5

1.3 Product overview and typical usage

YouWipe Erasure Tool 4 (called from now on in this document "Youwipe") is a software based secure data erasure solution. YouWipe can support a broad range of targeted devices. This includes hard disks such as HDDs, SSDs, flash drives such as USB data storage devices, SD cards, or mobile devices such as Android (higher than Android 5) or iOS based mobile phones and tablets. All these devices can be securely erased using the Youwipe solution. After performing the erasure of the target media, Youwipe performs the validation of the erasure results. At the end of the erasure action, it generates a report detailing the result and verdict of the erasure action.

In order to start using the product, the user needs to boot YouWipe from CD, USB or PXE server. The PXE server is a server installed on the local LAN, from which YouWipe can be booted by every computer connected to the LAN. Once YouWipe was booted, target media devices connected to the client computer on which the software is booted can be erased. Youwipe will trigger the erasure process by communicating with the controller on the target device. Through this communication, Youwipe will send commands of overwriting data with various patterns, both deterministic as well as random. The controller of the targeted media is responsible for executing the commands. The capability of the controller to correctly execute the overwriting actions is assumed to be in place, and the controller, as

[1] The version of the ST will be incremented by increasing the first decimal with 1 for each internal revision. External revisions (ex. To the scheme) are upgraded to the next increasing major version (ex. 1.0).

[2] Both Youwipe and WipeCenter are delivered to the customer as a single image. To validate the integrity of the image, a SHA256 checksum is separately delivered by Youwipe to the customer as described in Youwipe Erasure Tool User Manual v.2.0.6

well as all the hardware associated with the targeted media, are out of scope for the evaluation.

YouWipe lists all the detected hardware via its user interface (GUI). The user can choose from the options which disk to erase and which international erasure standard to employ. Erasure is performed by overwriting different patterns on the disk. Also depending on the used standard, overwriting can be performed multiple times. In the case of mobile phones, several erasure options are available, including (combinations of) overwrite, encryption and factory reset. Youwipe will interact with the controller of the mobile phone in order to launch these erasure actions. The controller, as well as the hardware of the mobile phone are assumed to be operating correctly and are out of scope of the evaluation.

After overwriting step, the data in disk is verified to be overwritten successfully. In order to verify, a percentage of the target media is checked against the last overwritten pattern. The verified percentage is always randomly chosen. In order to verify the data, Youwipe will retrieve the random data percentage by logical communication with the controller of the targeted media. The correct functionality of the controller in providing to Youwipe the erased locations asked, is assumed to be in place.

The result of the erasure is reported back to the user. The user has the option to save the report to a USB drive (in case the YouWipe software is booted via CD or USB) or to a local server (in case the YouWipe software is booted via the PXE server). In case the YouWipe software is booted via the PXE server, the erasure reports can be accessed and managed (reading and/or erasing, depending on the privilege level) via a report management console called WipeCenter 4 (called from now on in this document “WipeCenter”). The WipeCenter console is also in the scope of this evaluation.

There are three possible outcomes for an erasure report, which are either “erasure failed”, “erased with baseline security” or “erased with high security”. “Baseline security” level guarantees that user area was cleaned successfully and won't contain any user data but there can be inaccessible disk-specific areas where user data might still be found. “High security” level guarantees that all disk areas are erased and no user data can be found.

1.4 Secure erasure standards supported by the product

Youwipe supports the following erasure standards for the erasure of HDDs, SSD, SD cards or USB drives.

Erasure standard	Description
HMG Infosec Low	Overwrite 0x0 10% Verification of erased media
HMG Infosec High	Overwrite 0xAA Overwrite 0x55 Overwrite Random 10% Verification
DoD 5220.22-M	Overwrite 0x55 Overwrite 0xAA Overwrite Random 10% Verification
DoD 5220.22-M ECE	Overwrite 0x55 Overwrite 0xAA Overwrite Random

	Overwrite Full random Overwrite 0x55 Overwrite 0xAA Overwrite Random 10% Verification
SSD/ATA Baseline	Overwrite Random Secure Erase[3] Overwrite 0x55 10% Verification
SSD/ATA Enhanced	Overwrite Random Enhance Secure Erase[4] Overwrite 0x55 10% Verification
NIST SP 800/ATA Clear	Overwrite 0xFF 25% Verification
NIST SP 800/ATA Purge	Overwrite 0x55 Overwrite Random Overwrite 0xAA 25% Verification
Ext. HMG Infosec Low	DCO Restoration[5] HPA Expansion[6] Enhance Secure Erase Overwrite 0x0 10% Verification
Ext. HMG Infosec High	DCO Restoration HPA Expansion Enhance Secure Erase Overwrite 0xAA Overwrite 0x55 Overwrite Random 10% Verification
Ext. DoD 5220.22-M	DCO Restoration HPA Expansion Enhance Secure Erase Overwrite 0x55 Overwrite 0xAA Overwrite Random 10% Verification

[3] Secure Erase is the name given to a set of commands available from the firmware on PATA and SATA based hard drives. It is a firmware command that command the firmware to do an erasure

[4] The Enhanced version of the Secure Erase comment functions in a similar way as Secure Erase, with the difference that a more secure algorithm is used in the secure erase version

[5] DCO is an abbreviation for Device Configuration Overlay which is a hidden area on many of the HDD's used presently. The DCO Restoration function is mainly used to resize the number of sectors shown in the BIOS and OS (Operating System)

[6] HPA is an abbreviation for Host Protected Area, which is a hidden area that for example is used by computer manufacturers to preload an OS for installation and recovery.

Ext. DoD 5220.22-M ECE	DCO Restoration HPA Expansion Enhance Secure Erase Overwrite 0x55 Overwrite 0xAA Overwrite Random Overwrite Full random Overwrite 0x55 Overwrite 0xAA Overwrite Random 10% Verification
Ext. NIST SP 800/ATA Clear	HPA Expansion DCO Restoration Enhance Secure Erase Overwrite 0xFF 25% Verification
Ext. NIST SP 800/ATA Purge	HPA Expansion DCO Restoration Enhance Secure Erase Overwrite 0x55 Overwrite Random Overwrite 0xAA 25% Verification

Table 1 – Supported standards for the erasure of HDD, SSD, SD cards and USB drives medias

For the purposes of the evaluation, the erasure standard to be used is **Ext. HMG Infosec High**.

Youwipe 4.0 supports the following erasure methods for the erasure of mobile devices (iOS and Android).

Erasure method	Description
iOS	
Cryptographic erasure	Cryptographic erasure. Operating system reset and update to the latest. The erasure process overwrites the encryption key making the user data on the device inaccessible. The latest iOS operating system version is downloaded from the Apple servers and new encryption keys generated to the device during the erasure process. Overwriting is not necessary.
Android	
Factory reset	Android device built-in factory reset.
Infosec Low	Remove applications and writable files from the device flash memory. Overwrite the free space of the device's unprotected flash memory space two (2) times with random bytes.

	Perform Android device built-in factory reset.
Infosec High	Remove applications and writable files from the device flash memory. Overwrite the free space of the device's unprotected flash memory space three (3) times with random bytes. Perform Android device built-in factory reset.

Table 2 – Supported methods for the erasure of iOS and Android mobile devices

For the purposes of the evaluation, the erasure method to be used is

- **Infosec High** in case of Android mobile devices
- **Cryptographic erasure** in case of iOS mobile devices

1.5 TOE overview

1.5.1 TOE definition

The Target of Evaluation (TOE) described in this Security Target is the **Youwipe tool**, together with the **WipeCenter application** for the management of the generated erasure reports.

The **Youwipe tool** is responsible for:

- Generation of the random numbers used in the data erasure process
- Data erasing of the target device, based on the selected erasure standard or methodology
- Data erasure verification on the target device
- Audit data collection for the generation of the erasure report
- Erasure report generation and delivery (including saving the report on either an USB drive or the local server, as well as hashing the report to ensure its integrity)

The **WipeCenter application** is responsible for:

- Enforcing authentication for the access of erasure reports generated by the Erasure Engine of Youwipe, while at the same time collecting information about modifications to existing users and failed authentication attempts
- Ensuring role separation in the access of erasure report (separation between read-only rights and read-only + delete rights)
- Retrieving the erasure report from the local server and verifying its integrity
- Deleting erasure reports from the local server
- Generating new passwords for existing users

1.5.2 Security features not included in the TOE

The following security features are not included in the TOE:

- Booting of the Youwipe solution
- Booting of the WipeCenter application

1.5.3 Non-TOE Software and Hardware

The following software and hardware components are not part of the TOE, therefore will not be included in the evaluation activities.

Non-TOE software components:

- BIOS of the computer on which the Youwipe/WipeCenter solution is booted/installed
- Underlying Operating System of the machine on which WipeCenter is installed
- Java Virtual Machine running on the machine on which WipeCenter is installed
- Postgres database installed on the machine on which WipeCenter is installed

Non-TOE hardware components

- Computer system architecture on which the Youwipe/WipeCenter solution is installed
- USB drive, CD or PXE server from which the Youwipe solution is booted
- USB drive of local server on which the erasure report is saved
- Hard disk drives of the target media
- Hard disk controllers of the target media
- Hard disk controllers of the computing system on which the solution is booted

1.6 TOE Scope

1.6.1 TOE physical scope

Youwipe tool

The Youwipe tool is an image which can be booted on a machine. The Youwipe solution can be booted from a USB drive, CD, or PXE server.

WipeCenter application

The Wipecenter application resides as an installed application on the host computing machine, on top of the Java Virtual Machine.

1.6.1.1 The delivery process

The delivery process of the product is organized by developer in a form of an ISO image (including both Youwipe solution and WipeCenter application) through a web-portal. The ISO image is encrypted with AES-256 algorithm, the password to decrypt the file is sent to the customer via a separate communication channel. The link to download the file from the web-portal is sent to the customer. Moreover, the ISO image contains a SHA256 checksum for checking for any corrupt files during the download.

The available user documentation for the product is delivered in the same way through a web-portal.

1.6.2 TOE logical scope

Youwipe tool

The Youwipe tool is performing the secure erasure actions (in line with the selected standard), as well as verification of erasure results and issuing of the erasure report. The tool also provides a GUI which is used by the user to select the erasure target and algorithm. The Youwipe tool also generates the erasure report. The Youwipe tool includes all the tools and drivers needed for its interaction with other hardware elements on the host machine.

The interactions of the Youwipe tool with the other environmental components are as follows:

- The Youwipe tool interacts (via the driver) with the target media for erasure

- The Youwipe tool interacts (via the driver) with the BIOS of the host machine
- The Youwipe tool interacts with the external USB drive or server in order to save the generated erasure report

WipeCenter application

The WipeCenter application is responsible for regulating the access to the generated erasure reports. The application allows users to read or delete erasure reports stored on a local server. The WipeCenter application can only be used in case Youwipe is booted from a PXE server.

The interactions of the WipeCenter application with the other environmental components are as follows

- The WipeCenter application interacts with the Java Virtual Machine on the host machine in order to access the local machine BIOS, database or network connection (for importing erasure reports)

The interactions between TOE components and the environmental components are defined in the diagram below. **The TOE components are marked in the red (Youwipe) and green (WipeCenter) boxes**.

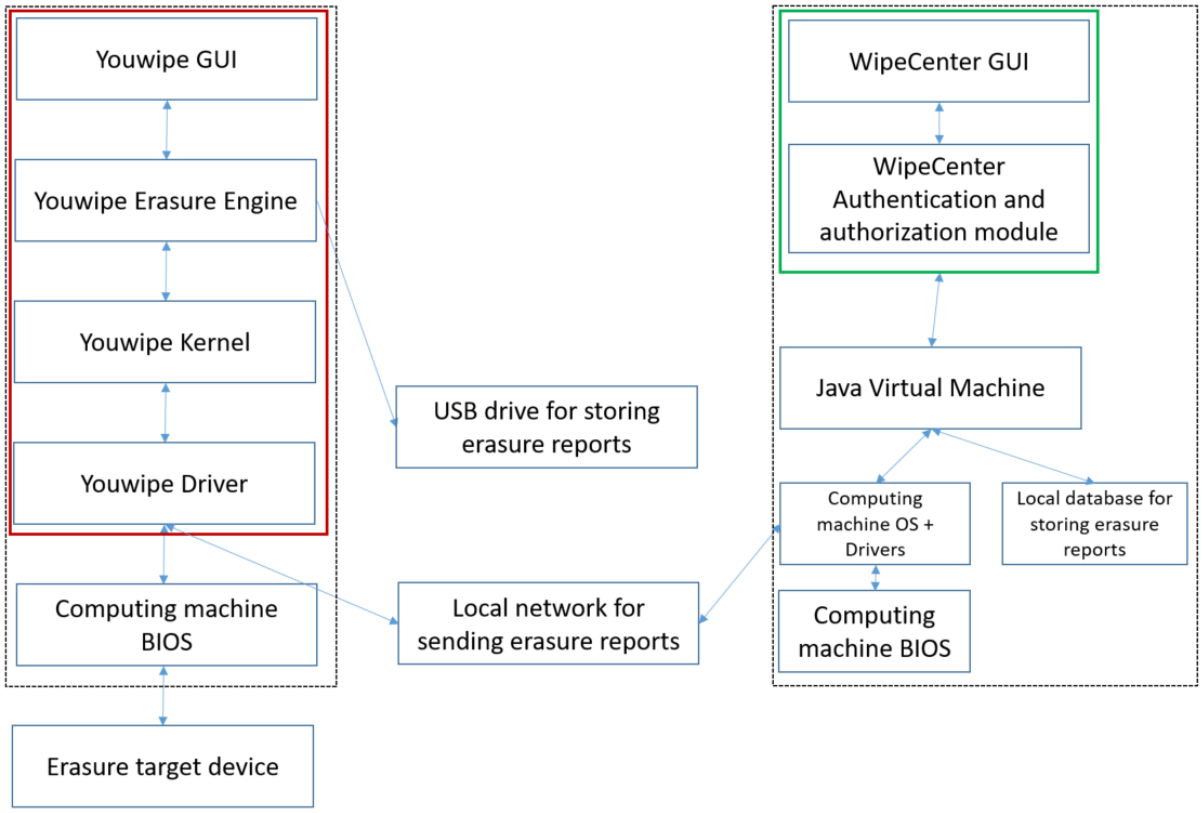


Figure 1 – Interactions of the solution's components

2 Conformance Claims

2.1 CC Version Conformance

This TOE is conforming to the Common Criteria for Information Technology Security, Version 3.1, Revision 5, April 2017.

2.2 CC Part 2 Conformance

This Security Target is CC Part 2 extended conformant.

2.3 CC Part 3 Conformance

This Security Target is CC Part 3 conformant.

2.4 Protection Profile Conformance

This Security Target (ST) has no Protection Profile (PP) to conform with.

2.5 Package Conformance

This Security Target is claims conformance to the EAL3 package of assurance requirements augmented with ALC_FLR.1.

2.6 Conformance Claim Rationale

There is no Conformance Claim Rationale for this ST.

3 Security Problem Definition

The following threats, organizational security policies and assumptions are considered for the TOE by the authors of this ST.

3.1 Threats

T.DATA_RECOVERY

An attacker who has access to the storage device after the data is erased is able to compromise the confidentiality of the original data stored on it, by recovering the data.

T.UNAUTHENTICATED_USER

An attacker is able to view and or delete the erasure reports through the network after bypassing or escalating the authentication mechanism of WipeCenter, which is the report management application, part of the TOE. This threat is applicable only when the TOE is booted from a PXE server and used within the network together with WipeCenter.

3.2 Organizational Security Policies (OSP)

P.AUDIT

The TOE will generate audit records (reports) containing information about the storage device`s erasure process.

P.REPORTS

The TOE will export reports in a manner that their integrity can be verified.

3.3 Assumptions

A.COMPETENT_USERS

The users (persons using the TOE) are competent, trained and they are following the user guidance documentation of the TOE.

A.BEHAVED_DRIVES

The storage devices aimed to be erased are well behaved, and expose the full storage capability to the operating system. In addition, the storage controllers of these devices are correctly passing the commands given by the Erasure Engine of Youwipe (erasure of certain location, collection of data from certain locations for validation).

A.BIOS_PREVENTING

The BIOS settings that can interfere with the erasing process by preventing the erasure are properly configured, hence not preventing the erasure process.

A.SYSTEM_TIME

The system time is properly set up, prior to start the erasure process, as it will be used for the auditing and reporting. The system time is collected from either the client machine's BIOS (for the Youwipe tool), or from the server machine's BIOS (for the WipeCenter application).

A.SECURE_LOCATION

The TOE will be used inside a secure location and physical custody will be maintained by an authorized person.

A.TRUSTED_NETWORK

The TOE will be deployed in a trusted network, assuming that there can be no malicious attacks on the TOE components coming from the interfaces connected to the network.

A.CORRECT_DEPLOYMENT

The TOE will be installed, configured and booted in a correct manner. This includes the correct configuration of the underlying operating system and Java Virtual Machine on the computer where the WipeCenter application is installed and run. Moreover, the image from which the product is booted is a correct, unmodified one. The Java Virtual Machine running on the machine where WipeCenter is installed comes from a trusted source, is properly installed and running. The Operating system of the machine where WipeCenter is installed comes from a trusted source, is properly installed and running, and free from malware.

A.WipeCenter_Random

The random numbers used by WipeCenter will originate from the Java Virtual Machine environment component and be used as such by WipeCenter. These quality (randomness) of these numbers is considered sufficient.

A.WipeCenter_Database

The Postgres database which is needed by WipeCenter in order to read/write elements such as usernames, passwords, roles, erasure reports, security logs, is properly installed, set-up and running on the machine where WipeCenter is installed.

3.4 Security Objectives

The following security objectives are to be satisfied by the TOE and its operational environment:

3.4.1 Security Objectives for the TOE

The following security objectives are to be satisfied by the TOE:

O.PROPER_ERASE

The TOE shall be able to erase all addressable data stored on selected storage device, making impossible any future data recovery on that device.

O.AUTHENTICATED_USER

The TOE shall provide means that only the users with valid credentials can access the erasure reports in order to view or delete these reports. The TSF shall also allow means for authenticated users to update their passwords. The TSF shall detect a number of failed authentication attempts and lock the authentication interface.

O.USER_SEPARATION

The TOE shall provide means to separate the users with different roles and capabilities such as viewing or deleting the erasure reports.

O.PROPER_AUDIT

The TOE shall provide means for security relevant events recording and supporting the user (person using TOE) with information about erasure standard, the status of the erasure, special area handling and areas that could not be erased.

O.PROPER_REPORTS

The TOE shall export reports containing information about the erasure process, guarantying the integrity of the data exported.

3.4.2 Security Objectives for the Operational Environment

OE.COMPETENT_USERS

The users (persons using TOE) will be competent, trained and they will follow the guidance documentation.

OE.BEHAVED_DRIVES

The only storage devices that are going to be erased by the TOE behave as expected and expose the full storage capability to the operating system. Moreover, the controllers of the target devices correctly pass the commands related to erasure and retrieval of erasure verification data.

OE.BIOS_PREVENTING

The BIOS settings that can interfere with the erasing process will be properly configured, hence not preventing the erasure process.

OE.SYSTEM_TIME

The operational environment will provide correct system time.

OE.SECURE_LOCATION

The location where TOE will be used will be a secure one, and the network where the TOE will be deployed will be trusted (including trusted network users).

OE.CORRECT_DEPLOYMENT

The operational environment will ensure that the TOE can be installed, configured and run according to the vendor's installation guidance. This will include the correct installation of the underlying operating system and Java Virtual Machine on the computer where WipeCenter is installed.

OE.WipeCenter_Random

The operational environment will ensure that the TOE (WipeCenter) receives random numbers.

OE.WipeCenter_Database

The operational environment will provide the database necessary for the operation of WipeCenter

3.4.3 Security Objectives Rationale

Table 3 - Security Objectives Rationale

	O.PROPER_ERASE	O.AUTHENTICATED_USER	O.USER_SEPARATION	O.PROPER_AUDIT	O.PROPER_REPORTS	OE.COMPETENT_USERS	OE.BEHAVED_DRIVES	OE.BIOS_PREVENTING	OE.SYSTEM_TIME	OE.SECURE_LOCATION	OE.CORRECT_DEPLOYMENT	OE_WipeCenter_Random	OE_WipeCenter_Database
T.DATA_RECOVERY	X												
T.UNAUTHENTICATED_USER		X	X										
P.AUDIT				X									

P.REPORTS					**X**								
A.COMPETENT_USERS						**X**							
A.BEHAVED_DRIVES							**X**						
A.BIOS_PREVENTING								**X**					
A.SYSTEM_TIME									**X**				
A.SECURE_LOCATION										**X**			
A.TRUSTED_NETWORK										**X**			
A.CORRECT_DEPLOYMENT											**X**		
A.WipeCenter_Random												**X**	
A.WipeCenter_Database													**X**

The threat **T.DATA_RECOVERY** is countered (mitigated) by TOE security objective **O.PROPER_ERASE**. TOE security objective O.PROPER_ERASE ensures that the TOE will overwrite completely the content of the specified storage device.

The threat **T.UNAUTHENTICATED_USER** is countered (mitigated) by TOE security objective **O.AUTHENTICATED_USER** and **O.USER_SEPERATION**. O.AUTHENTICATED_USER ensures that only authenticated users have access to the WipeCenter functionality of the TOE. O.USER_SEPERATION aims that the role separation between the users are enforced.

The OSP **P.AUDIT** is enforced by TOE security objective **O.PROPER_AUDIT**. TOE security objective O.PROPER_AUDIT, ensures that specified security relevant events will be recorded in order to monitor the whole process.

The OSP **P.REPORTS** is enforced by TOE security objective **O.PROPER_REPORTS**. This will ensure that all data collected by the audit component will be exported and will use an integrity checking mechanism to ensure exported data integrity.

The assumption **A.COMPETENT_USERS** is upheld by environment security objective **OE.COMPETENT_USERS**. This ensures that only competent and trained users (persons using TOE) will operate TOE as per provided guidance documentation.

The assumption **A.BEHAVED_DRIVES** is upheld by environment security objectives **OE.BEHAVED_DRIVES**. This ensures that storage devices targeted to be erased will be well behaved and expose the full storage capability to the operating system. Moreover, the controllers on the target devices will correctly pass the commands of erasure and retrieval of data.

The assumption **A.BIOS_PREVENTING** is upheld by environment security objective **OE.BIOS_PREVENTING**.
This ensures that the BIOS settings that can interfere with the erasing process will be properly configured by the users (persons using TOE) in such a way to not prevent the process.

The assumption **A.SYSTEM_TIME** is upheld by environment security objective **OE.SYSTEM_TIME**. This ensures that the system time will be properly set up by the user (person using TOE), prior to the start the erasure, and the audit component will obtain reliable timestamps.

The assumption **A.SECURE_LOCATION** is upheld by environment security objective **OE.SECURE_LOCATION**. This will ensure that the TOE will be used only in controlled access areas and physical custody will be maintained by an authorized person.

The assumption **A.TRUSTED_NETWORK** is upheld by environment security objective **OE.SECURE_LOCATION**. This will ensure that the TOE will be deployed only in a trusted network environment, protecting against malicious attacks on network connected interfaces.

The assumption **A.CORRECT_DEPLOYMENT** is upheld by the environment security objective **OE.CORRECT_DEPLOYMENT**. This will ensure that the TOE will be installed and booted according to the vendor's guidance, moreover the underlying operating system and Java Virtual Machine on the computer which hosts WipeCenter will be setup properly and free from malware.

The assumption **A.WipeCenter_Random** is upheld by the environment security objective **OE.WipeCenter_Random**. This will ensure that the TOE will receive random numbers from the operational environment.

The assumption **A.WipeCenter_Database** is upheld by the environment security objective **OE.WipeCenter_Database**. This will ensure that the TOE (WipeCenter part) will be installed on a machine where a database is installed and correctly running.

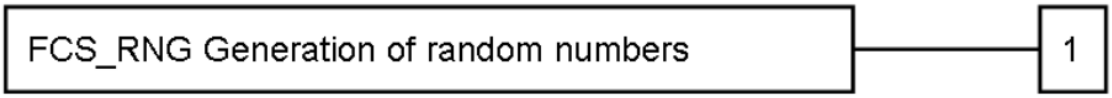
4 Extended Components Definition

4.1 Extended family FCS_RNG

An additional family (FCS_RNG) is defined in this Security Target, in order to provide relevant security functional requirements to the TOE. The family is included within the class FCS (Cryptographic Support), due to the fact that the random numbers are a major component in building up cryptographic algorithms and functions. This additional family describes the functional requirements needed for

random number generation. The additional family definition is taken from [PP0084], a certified Protection Profile used for the evaluation of security IC platforms. As the random number generation function defined by this family is considered sufficient to satisfy the random number generation needs for the TOE, full re-use is made of the FCS_RNG family definition in [PP084].

The family contains a single component, FCS_RNG.1.



4.1.1 Extended component FCS_RNG.1

The definition of the FCS_RNG.1 component, as taken from [PP084], is considered for this ST.

FDP_RNG.1	**Random number generation**
Hierarchical to:	No other components
Dependencies	No dependencies
FCS_RNG.1.1	The TSF shall provide a [selection: *physical, non-physical true, deterministic, hybrid physical, hybrid deterministic*] random number generator that implements: [assignment: *list of security capabilities*]
FCS_RNG.1.2	The TSF shall provide [selection: *bits, octets of bits, numbers [assignment: format of the numbers]*] that meet [assignment: *a defined quality metric*]

5 Security Requirements

5.1 Security Functional Requirements

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 is made unavailable upon the [**deallocation of resources from**] the following objects: [**storage device in the scope of the solution**]

FIA_UAU.2	**User authentication before any action**
Hierarchical to:	FIA_UAU.1 Timing of authentication
Dependencies	FIA_UID.1 Timing of identification
FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FMT_SMR.1	**Security roles**
Hierarchical to:	No other components
Dependencies	FIA_UID.1 Timing of identification

FMT_SMR.1.1	The TSF shall maintain the roles: [**WipeCenter Administrator, WipeCenter User, Youwipe User**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles

FMT_MTD.1	**Management of TSF data**
Hierarchical to:	No other components
Dependencies	FMT_SMR.1 Security Roles FMT_SMF.1 Specification of Management Functions
FMT_MTD.1.1	The TSF shall restrict the ability to [**change_default**] the [**WipeCenter Admin password, WipeCenter User password**] to [**WipeCenter Admin, WipeCenter User**].

FMT_SMF.1	**Specifications of Management Functions**
Hierarchical to:	No other components
Dependencies	No dependencies
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**change WipeCenter users password**].

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: a) Start-up and shutdown of the audit functions; b) All auditable events for the [**not specified**] level of audit; and c) [**erasure process events, updates to users passwords in WipeCenter, unsuccessful authentication attempts in WipeCenter**].
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of the 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 PP/ST, [**target device identification, disk identification, internal id, model info, manufacturer info, total number of sectors, sector size, overwrite standard/method, verification percentage, number of sector read/write errors, date and time operation was started, date and time operation was completed, erasure level achieved**].

FPT_ITI.1	**Integrity of exported TSF data**
Hierarchical to:	No other components

Dependencies	No dependencies
FPT_ITI.1.1	The TSF shall provide the capability to detect modifications of all TSF data during transmission between the TSF and another trusted IT product within the following metric [**SHA256 digest**].
FPT_ITI.1.2	The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and another trusted IT product and perform [**clear warning to the user**] if modifications are detected.

FIA_UID.1	**Timing of identification**
Hierarchical to:	No other components
Dependencies	No dependencies
FIA_UID.1.1	The TSF shall allow [**no actions**] on behalf of the user to be performed before the user is identified.
FIA_UID.1.2	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

FIA_AFL.1	**Authentication failures**
Hierarchical to:	No other components

Dependencies	FIA_UAU.1 – Timing of authentication
FIA_AFL.1.1	The TSF shall detect when [**3**] unsuccessful authentication attempts occur related to [**authentication of WipeCenter Administrator, WipeCenter User in WipeCenter**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [**reached**], the TSF shall [**block access to WipeCenter for the particular user account**].

FCS_RNG.1	**Random number generation**
Hierarchical to:	No other components
Dependencies	No dependencies
FCS_RNG.1.1	The TSF shall provide a [**deterministic**] random number generator that implements: [**generation of random bytes for usage within data overwriting actions**]
FCS_RNG.1.2	The TSF shall provide [**octets of bits**] that meet [**random bytes with a probability of 2^{-8} of occurring**]

FCS_COP.1//SHA256	**Cryptographic Operation**
Hierarchical to:	No other components

Dependencies	FDP_ITC.1 – Import of user data without security attributes Or FDP_ITC.2 – Import of user data with security attributes Or FCS_CKM.1 – Cryptographic key generation, FCS_CKM.2 – Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [**hash value calculation**] in accordance with a specified cryptographic algorithm [**SHA256**] and cryptographic key sizes [none] that meet the following: [[**FIPS 180-4] for SHA256**].

FCS_COP.1//Bcrypt	**Cryptographic Operation**
Hierarchical to:	No other components
Dependencies	FDP_ITC.1 – Import of user data without security attributes Or FDP_ITC.2 – Import of user data with security attributes Or FCS_CKM.1 – Cryptographic key generation, FCS_CKM.2 – Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [**hash value calculation**] in accordance with a specified cryptographic algorithm [**Bcrypt**] and cryptographic key sizes [none] that meet the following: [**[Bcrypt] for Bcrypt**].

FCS_COP.1//RSA_sign	**Cryptographic Operation**
Hierarchical to:	No other components
Dependencies	FDP_ITC.1 – Import of user data without security attributes Or FDP_ITC.2 – Import of user data with security attributes Or FCS_CKM.1 – Cryptographic key generation,

	FCS_CKM.2 – Cryptographic key destruction
FCS_COP.1.1	The TSF shall perform [**generation and verification of digital signature**] in accordance with a specified cryptographic algorithm [**RSA signature scheme with appendix according to [PKCS#1]**] and cryptographic key sizes [**2048**] that meet the following: [**[PKCS#1]**].

5.2 Security Assurance Requirements

EAL3 (methodically tested and checked) package augmented with ALC_FLR.1 component is the assurance level claimed for the TOE. The ALC_FLR.1 component is adding assurance for systematic flaw remediation.

REQUIREMENT CLASS	REQUIREMENT COMPONENT	
ADV	**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
	AGD_PRE.1	Preparative Procedures
ALC: Life-cycle support	**ALC_CMC.3**	Authorization controls
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.1	Flaw remediation
	ALC_LCD.1	Developer defined life-cycle model
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	OE summary specification
ATE: Tests	**ATE_COV.2**	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
AVA: Vulnerability assessment	**AVA_VAN.2**	Vulnerability analysis

5.3 Security Functional Requirements Rationale

	FAU_GEN.1	FDP_RIP.1	FPT_ITI.1	FIA_UAU.2	FMT_SMR.1	FCS_RNG.1	FIA_UID.1	FMT_MTD.1	FMT_SMF.1	FCS_COP.1//SHA256	FCS_COP.1//Bcrypt	FCS_COP.1//RSA_sign	FIA_AFL.1
O.PROPER_AUDIT	X												
O.PROPER_ERASE		X				X							
O.PROPER_REPORTS			X							X		X	
O.AUTHENTICATED_USER				X			X	X	X		X		X
O.USER_SEPERATION					X								

The TOE security objective **O.PROPER_AUDIT** is enforced by TOE security functional requirement **FAU_GEN.1**. TOE SFR FAU_GEN.1 ensures that the security objective O.PROPER_AUDIT is satisfied by requiring TSF to define the level of auditable events and clearly specifying the security relevant events that will be recorded.

The TOE security objective **O.PROPER_ERASE** is enforced by TOE security functional requirements **FDP_RIP.1** and **FCS_RNG.1**. TOE SFR FDP_RIP.1 ensures that the security objective O.PROPER_ERASE is satisfied by requiring that any residual information content from the resource (original user data) will be made unavailable at deallocation of the resource from the targeted storage device. SFR FCS_RNG.1

ensures that the security objective O.PROPER_ERASE is satisfied by requiring the TSF to have the capability to generate random numbers of a certain quality metric, to be used in the data overwriting steps that rely on random number overwrite.

The TOE security objective **O.PROPER_REPORTS** is enforced by TOE security functional requirements **FPT_ITI.1, FCS_COP.1//SHA256** and **FCS_COP.1//RSA_sign**. TOE SFR FPT_ITI.1 ensures that the security objective O.PROPER_REPORTS is satisfied by requiring TSF to provide the capability to detect modification of all TSF data during report transmission, using SHA256 digest. It also performs the assignment of clearly informing the user when integrity modification is detected. FCS_COP.1//SHA256 defines the functionality of the SHA256 hashing algorithm, creating a SHA digest on the generated erasure reports. FCS_COP.1//RSA_sign defines the generation of digital signatures on the created erasure reports. The report is signed with a private key hardcoded in the binary of the Youwipe tool, while the signature is verified with the public key hardcoded in the binary of the WipeCenter application.

The TOE security objective **O.AUTHENTICATED_USER** is enforced by TOE security functional requirements **FIA_UAU.2, FMT_MTD.1, FMT_SMF.1, FCS_COP.1//Bcrypt, FIA_AFL.1** and **FIA_UID.1**. FIA_UAU.2 ensures that the security objective O.AUTHENTICATED_USER is satisfied by requiring each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.1 ensures that the security objective is satisfied by requiring each user to be identified before allowing any TSF-mediated actions to be performed on behalf of the user. FIA_AFL.1 ensures that the TSF will lock access to Youwipe for a user account after 2 incorrect authentication attempts. Finally, FMT_MTD.1 and FMT_SMF.1 allows users of WipeCenter to update their passwords and FCS_COP.1//Bcrypt allows for the new passwords to be hashed before being stored.

The TOE security objective **O.USER_SEPERATION** is enforced by TOE security functional requirement **FMT_SMR.1**. FMT_SMR.1 ensures that the security objective O.USER_SEPERATION is satisfied by requiring TSF to provide security roles and recognizing these roles with respect to security.

5.4 SFR Component Dependencies Rationale

This section describes how security functional requirements component dependencies are satisfied and the corresponding rationale.

Security Functional Requirements	**Dependencies**	**Rationale**
FAU_GEN.1 (Audit data generation)	FPT_STM.1 (Time Stamps)	Not satisfied by TOE. Date and time is provided by TOE environment (OE.PROPER_TIME)
FIA_UAU.2 (User authentication before any action)	FIA_UID.1 (Timing of identification)	Satisfied by the security function SF.MANAGEMENT_CENTER. This security function allows users to claim their identity in the form of a username.
FMT_SMR.1 (Restrictions on security roles)	FIA_UID.1 (Timing of identification)	Satisfied by the security function SF.MANAGEMENT_CENTER. This

		security function allows users to claim their identity in the form of a username.
FCS_COP.1//SHA256(Cryptographic operation)	FDP_ITC.1 – (Import of user data without security attributes) Or FDP_ITC.2 – (Import of user data with security attributes) Or FCS_CKM.1 – (Cryptographic key generation), FCS_CKM.2 – (Cryptographic key destruction)	Not satisfied by the TOE. FCS_COP.1 is used for defining the SHA256 hashing function. The generation or destruction of keys is not applicable for this SFR.
FCS_COP.1//Bcrypt (Cryptographic operation)	FDP_ITC.1 – (Import of user data without security attributes) Or FDP_ITC.2 – (Import of user data with security attributes) Or FCS_CKM.1 – (Cryptographic key generation), FCS_CKM.2 – (Cryptographic key destruction)	Not satisfied by the TOE. FCS_COP.1 is used for defining the Bcrypt hashing function. The generation or destruction of keys is not applicable for this SFR.
FCS_COP.1//RSA_sign (Cryptographic operation)	FDP_ITC.1 – (Import of user data without security attributes) Or FDP_ITC.2 – (Import of user data with security attributes) Or FCS_CKM.1 – (Cryptographic key generation), FCS_CKM.2 – (Cryptographic key destruction)	Not satisfied by the TOE. The public-private key pair used for the digital signing of the erasure reports is embedded in the Youwipe and WipeCenter binaries. The keys are not generated by the TOE and are not destroyed.
FMT_MTD.1 (Management of TSF data)	FMT_SMR.1 (Security roles)	Satisfied by the security function SF.MANAGEMENT_CENTER. This

	FMT_SMF.1 (Specification of management functions)	security function allows users to update their WipeCenter password.
FIA_AFL.1 (Authentication Failure Handling)	FIA_UAU.1 (Timing of Authentication)	Satisfied by TOE, through the claimed SFR FIA_UAU.2

5.5 Security Assurance Requirements Rationale

EAL3 evaluation assurance level augmented with ALC_FLR.1 (EAL3 + ALC_FLR.1) has been chosen in order to comply with market exigencies for this typology of products. This evaluation assurance levels is expected to provide to the customers a comfortable level of assurance that is consistent with today's good practices and industry standards.

A comfortable level of assurance is obtained by combining SARs requiring:

- Review of the TOE design
- Review of the TOE guidance
- Review of the TOE's development controls, including configuration management, secure delivery and flaw remediation
- Review of TOE's developer testing process
- Validation of TOE's robustness against relevant attacks, up to the level of AVA_VAN.2 (Basic attack potential)

Moreover, the EAL3+ assurance level is chosen also in relation with similar products evaluated against Common Criteria. By researching similar products evaluated and listed on the Common Criteria portal (https://www.commoncriteriaportal.org/products/#DP), it is concluded that similar data erasure tools are evaluated against EAL3+ or lower level of assurance.

6 TOE Summary Specification

6.1 Security Functions

SF.PROCESS_CONTROLLER

The SF.PROCESS_CONTROLLER function of the TOE enforces the **FAU_GEN.1** and **FPT_ITI.1** requirements.

FAU_GEN.1 requires a reliable timestamp, which is provided by the Operating System on which the TOE is booted. The correct date and time information is taken by Operating System from the BIOS at the booting time. Audit data is generated every time when wiping data storage devices. The output of these actions are stored by the TOE in the form of audit reports. Along with the success or failure of events being recorded, the TSF records also info about TOE identification, disk identification, overwrite pattern, number of passes and write failures, date and time when the operation was started, date and time when the operation was completed, evaluation level achieved.

Moreover, the TOE generates audit data regarding unsuccessful login attempts (timestamp, username, reason for failer authentication – username/password failed) on WipeCenter, as well as allows changes to the passwords of the users in WipeCenter (and logging them).

Audit data is also generated for the start-up and shutdown of audit. The audit functions available to the user (person using TOE) cannot be disabled and are run automatically.

After the erasing process, the TOE is verifying the conformity of the erasure process results and the reporting data collected is evaluated for modification during transmission as per FPT_ITI.1 security functional requirement, by SHA256 digest and the user is clearly alerted if any integrity issue is found. The SHA256 digest is generated based on the FCS_COP.1//SHA256 SFR. The signature of the erasure report is performed based on FCS_COP.1//RSA_sign. The information about potential integrity issues can be identified by the user within the generated erasure report in the field “Report signature” as a failed status. During the erase verification process, if any nonconformity is detected, the TOE will report that erasure process has failed and the storage device has not been fully erased.

SF.SECURE_ERASE

This security function is coming to fulfil the requirements of **FDP_RIP.1** security functionality. TOE erases existing data by overwriting it (in the evaluated configuration) using the Ext. HMG Infosec High erasure standard (please refer to Table 1 for the description of this erasure standard).

SF.MANAGEMENT_CENTER

The SF.MANAGEMENT_CENTER function of the TOE enforces the **FIA_UAU.2** (User authentication before any action), **FMT_MTD.1** (Management of TSF data), **FMT_SMF.1** (Specification of management functions), **FMT_SMR.1** (Security roles), and **FCS_COP.1//Bcrypt** (Hashing). SF.MANAGEMENT_CENTER allows only authenticated users to have access to the WipeCenter application when the TOE is booted from a PXE server. Users need to authenticate using a username and password in order to be able to access and manage erasure reports. The WipeCenter application creates a differentiation between Administrator and User roles. The User role is able to retrieve and read erasure reports, while the Administrator is able in addition to erase certain reports. Authenticated users can update their own passwords, which are then stored in a hashed form, using the Bcrypt hash function. The same security feature enforces the FIA_AFL.1 (Authentication failure handling), through which the user account will be blocked after 3 incorrect authentication attempts.

SF.MANAGEMENT_CENTER also enforces users with different roles to have different capabilities hence a role separation between different user roles.

FIA_UAU.2 and FMT_SMR.1 have a dependency (**FIA_UID.1**) that requires users to be successfully identified before allowing certain TSF-mediated actions on behalf of that user. The SF.MANAGEMENT_CENTER security function allows users of the TOE to claim their identity in the form of a username, hence fulfilling this dependency requirement.

SF.RANDOM_NUMBERS

This function is coming to fulfil the requirements of FCS_RNG.1 security functionality. The TOE generates random numbers of a certain quality metric, in order to use them in the data overwriting process.

6.2 TOE Summary Specification Rationale

This section identifies the Security Functions provided by the TOE, mapped to the Security Functional Requirements contained in this Security Target (ST).

Security Functions	Security Functional Requirements
SF.PROCESS_CONTROLLER	FAU_GEN.1 - Audit data generation
	FCS_COP.1//SHA256 – Cryptographic operation
	FCS_COP.1//Bcrypt – Cryptographic operation
	FCS_COP.1//RSA_sign – Cryptographic operation
	FPT_ITI.1 - Integrity of exported TSF data
SF.SECURE_ERASURE	FDP_RIP.1 - Subset residual information protection
SF.MANAGEMENT_CENTER	FIA_UAU.2 - User authentication before any action
	FMT_SMR.1 - Restrictions on security roles
	FIA_UID.1 - Timing of identification
	FMT_MTD.1 – Management of TSF Data
	FMT_SMF.1 – Specification of Management Functions
	FIA_AFL.1 – Authentication failure handling
SF_RANDOM_NUMBERS	FCS_RNG.1 – Random number generation

6.3 TOE's protection against interference and logical tampering

The TOE protects TSF data against interference and logical tampering through the following items:

- The security function SF_PROCESS_CONTROLLER ensures that the TOE attaches a hash digest to the erasure reports, after generating the reports. In this way, the integrity of the reports can be validated each time a report is being retrieved from the storage server.
- The assumption A.SECURE_LOCATION ensures that the TOE will be used in a secure, trusted environment. The elements of the operational environment necessary for the TOE's execution are stored within the secure location, and no TSF data is at any point transferred outside of the

secure location. Therefore, this ensures the TOE's protection against interference and logical tampering.

6.4 TOE's protection against security functionality bypass

The TOE protects itself against security functionality bypass through the following items:

- The assumption A.CORRECT_DEPLOYMENT ensures that the product is installed and run based on the provided vendor guidance
- Once the product is successfully booted, there are no security features which could be bypassed. The generation of an erasure report requires a successful operation of erasure (which in turn relies on the generation of random numbers), while accessing/modifying a stored erasure report requires a correct user authentication step.

Abbreviations

CM	Configuration Management
EAL	Evaluation Assurance Level
GUI	Graphical User Interface
TOE	Target of Evaluation
TSF	TOE Security Functionality
RNG	Random Number Generator
ST	Security Target
PXE	Preboot Execution Environment

Glossary of terms

PXE Server	Preboot Execution Environment server, offering booting capabilities to client computers which are configured to boot from one of its network devices
SHA256 digest	Hash value resulted after hashing a input message based on the SHA256 hashing algorithm

References

[PP084] Security IC Platform Protection Profile with Augmentation Packages, Version 1.0

[FIPS 180-4] FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Secure Hash Standard (SHS), August 2015

[Bcrypt] A Future-Adaptable Password Scheme, Niels Provos, David Mazieres

[PKCS#1] RSA Cryptography Specifications Version 2.2