SecureAge

SecureData 8.0 Security Target

Common Criteria: EAL2+ ALC_FLR.2

Document Version : 1.0

Document Date : 12-APR-2023

Document management

Document identification

Document title	SecureData 8.0 Security Target
Document version	1.0
Document date	12-APR-2023
Release Authority	Hendy

Document history

Version	Date	Description
0.1	09-JUNE-2020	Released for internal review
1.0	12-APR-2023	Update content based on CB feedback.

Table of Contents

1 Security Target Introduction 5

1.1 ST Reference 5

1.2 TOE Reference 5

1.3 Document organization 5

1.4 Defined terms 6

1.5 TOE Overview 7

1.5.1 TOE Usage and major security functions 7

1.5.2 TOE Type 8

1.5.3 Non-TOE Supporting Hardware, Software and/or Firmware 9

1.6 TOE Description 10

1.6.1 Presentation of TOE 10

1.6.2 Physical scope of the TOE 11

1.6.3 Logical scope of the TOE 14

1.7 Evaluated Configuration 14

2 Conformance Claim 15

3 Security Problem Definition 16

3.1 Overview 16

3.2 Threats 16

3.3 Organisational security policies 16

3.4 Assumptions 16

4 Security Objectives 18

4.1 Overview 18

4.2 Security Objectives for the TOE 18

4.3 Security Objectives for the TOE Operational Environment 18

4.4 Security Objectives Rationale 20

4.4.1 TOE Security objectives rationale 21

4.4.2 Environment security objectives rationale 21

5 Extended Components Definition 23

6 Security Requirements 24

6.1 Overview 24

6.2 Security functional requirements 24

6.2.1 Overview 24

6.2.2 FCS_COP.1 Cryptographic operation 25

6.2.3 FCS_CKM.1 Cryptographic key generation 26
6.2.4 FCS_CKM.4 Cryptographic key destruction 26
6.2.5 FPT_FLS.1 Failure with preservation of secure state 26
6.2.6 FRU_FLT.1 Degraded fault tolerance 26
6.3 TOE Security assurance requirements 27
6.4 Security requirements rationale 28
6.4.1 Dependency rationale 28
6.4.2 Mapping of SFRs to security objectives for the TOE 29
6.4.3 Explanation for selecting the SARs 30
7 TOE Summary Specification 31
7.1 Overview 31
7.2 File encryption 31
7.3 Fault tolerance 32
8 Reference 33

1 SECURITY TARGET INTRODUCTION

1.1 ST Reference

Doc Title	SecureData 8.0 Security Target
Doc Version	1.0
Doc Date	12-APR-2023

1.2 TOE Reference

TOE Title	SecureData
TOE Version	8.0

1.3 Document organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 22 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 33 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 44 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 05 provides the extended components definition for the TOE (ASE_ECD.1).
- Section 66 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).
- Section 7 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 Defined terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term	Description
TSF data	Data affect the operation of the TOE upon which the enforcement of the SFR relies, which include: • SecureData configuration data
TOE user	Individual who is authorised to use the TOE.
Administrator	Individual who is responsible for the TOE policy configuration, installation and maintenance. He/she has Windows OS administrator privilege.

1.5 TOE Overview

SecureData is one of the tools of SecureAge Security Suite (Suite), it provides user endpoint automatic file and folder encryption for seamless security of all user files without sacrificing productivity or breaking established norms and practices. SecureData helps to enforce data security requirements in preventing data loss and data leakage of sensitive personal information and valuable enterprise information assets. The Suite is an endpoint license-based application, which provides the essential components necessary for complete protection against intentional or accidental data loss or breach. The Suite needs to be installed as one application, it comprises 4 components (SecureData, SecureFile, SecureDisk and SecureEmail), each component is able to be activated individually by providing valid license code.

1.5.1 TOE Usage and major security functions

The major security function of SecureData is to provide automatic encryption for user data/file(s) regardless of its storage media. Any data/file(s) that are created, edited, moved or copied to any local, external or network storage devices, such as fileserver, are automatically encrypted based on pre-defined policies. Even local drive of a machine is shared across the network, the transmission of the user data/file(s) will remain encrypted over the network and only authorized recipients could decrypt the data/file(s). Refer to Section 1.6.3 for details of file encryption/decryption process.

There are 2 types of TOE usage:

1. Normal file operation, the TOE is designed and registered as one of Windows OS system driver, each time when user conduct the operation, such as read, write, copy, Windows OS will invoke TOE to complete the operation. This usage is integrated into Windows file operation process, without changing the user method of use toward their computers, transparently ensures all important data/file(s) are stored in encrypted format.
2. Background encryption, it refers to operation of file sharing, initial background encryption after TOE successful installation and manual encryption. Different from normal file operation, user need to invoke TOE via right click menu in Windows (initial background encryption is automatic trigger after user SecureAge profile has been created). During this usage, if there is a power failure or physical anomaly inflicting temporary failure of disk operation, only the temporary file created by TOE will be affected or corrupted, which is to protect the original file.

The following table highlights the range of security functions implemented by the TOE.

Table 1: TOE Security Functions

Security Function	Description
File Encryption	TOE provides data/file(s) encryption using the AES algorithm with each data/file(s) protected by a different randomly generated 256-bits AES Session Key.

Security Function	Description
Fault Tolerance	TOE maintains the secure state during TOE failure to operate (e.g., background encryption) on the user data/file(s) stored in the local drives. If there is a power failure or physical anomaly inflicting temporary failure of disk operation during the process of TOE background encryption, only the temporary data/file(s) which is currently processing will be affected or corrupted.

1.5.2 TOE Type

SecureData is a software-based security product for Microsoft Windows Operating System based desktop or computer platform that provides transparent encryption for user data/file(s) regardless of its storage media. Any data/file(s) that are created, edited, moved or copied to any local, external or network storage devices are automatically encrypted based on pre-defined policies.

1.5.3 Non-TOE Supporting Hardware, Software and/or Firmware

Table 2: Minimum System Requirements for TOE

Minimum System Requirements	
Operating Systems	Microsoft Windows 10
Processor	x86/x64 architecture
Memory (RAM)	1 GB
Hard disk	300MB
Application	SecureAge Security Suite 8.0.x Remarks: On top of 4 separate components (SecureData, SecureFile, SecureDisk and SecureEmail), SecureAge Security Suite provide some shared general functions, they are not within this evaluation. Below are the general security functions provided by Suite and needed for TOE operation. • Identification & Authentication • Key generation Refer to Section 1.7 of this document for any specific setup requirement for Suite.

1.6 TOE Description

1.6.1 Presentation of TOE

As TOE is part of Suite and cannot work independently, this section presents TOE as one of components of Suite. TOE functions on supported Windows OS defined in section 1.5.3, provides transparent encryption for user data/file(s) regardless of its storage media. After Suite has been installed and SecureData license has been activated in user computer, few more steps need for user to use TOE security function:

Create SecureAge user profile

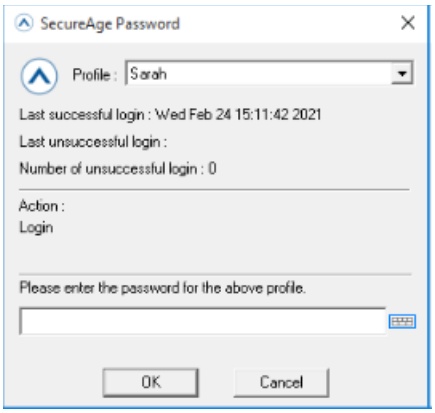
During this process, each user will be equipped with:

- One or more RSA key pair(s) (new generate or import) and AES key.
- User credential, either password or hardware token, which is used to login Suite.

SecureAge user profile creation is handled by Suite, not within TOE evaluation scope but necessary to support TOE operation.

Login Suite

Each time user login Windows, user needs to login SecureAge Security Suite separately via the login page as below:



User needs to input their SecureAge user profile credential or insert hardware token, only after successfully login Suite, the TOE security function is ready to use.

SecureAge Security Suite login is handled by Suite, not within TOE evaluation scope but necessary to support TOE operation.

After successfully login Suite, user is able to conduct the file operation as normal, Windows will invoke SecureData driver during this process, which is the TOE security function. Refer to below section 1.6.2 and 1.6.3 of this document for more details.

Logout Suite

After successfully logout Suite, TOE will destroy AES key from Windows Kernel Memory. and user not able to operate encrypted file anymore.

1.6.2 Physical scope of the TOE

A typical implementation of the TOE can be found in Figure 1 below, in which identify the various components requires in the TOE deployment architecture, those components highlighted in **GREY** is the scope of the TOE.

Note that, all underlying operating system and the hardware components describe in this document shall be treated as not part of the TOE scope. The components are not part of the TOE scope defined in Section 1.5.3.

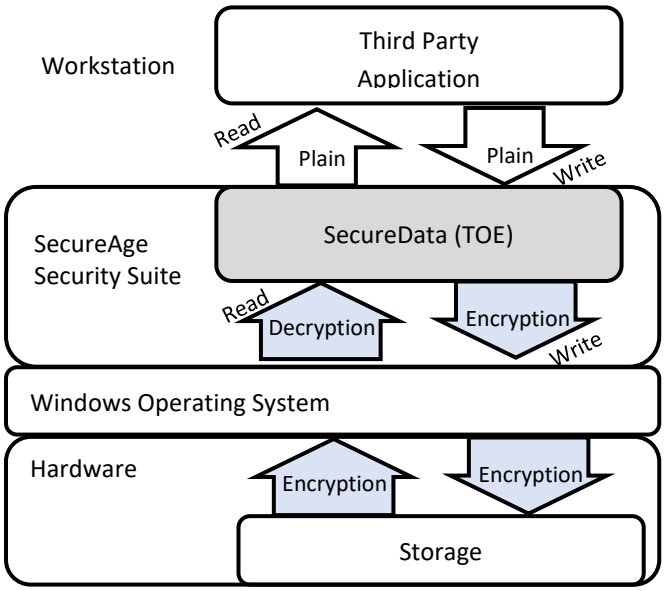


Figure 1 – TOE

Below is the TOE evaluation scope:

The physical deliverable of the TOE comprised of the following items:

1. TOE software installation file (SecureAge Security Suite installation package) delivered to the customer in the form of CD or unique download link: https://files.secureage.com/SecureAge_8.0.17_OTA2Cg==.zip

Unique Identifier	Version	Method of delivery
SecureAge Security Suite Installation Package	8.0.7	CD or download link

The files and their respective hashes in the installation package are listed below:

Filename	**SHA 256**
autoconf.ini	93a15db1597987f259eef01d7a55dd8244e540cfcc93ffd97d4460de89f69785
CusWiz64.exe	33c2ec9d61a66be4fd15d6556342988e0b9413de786252632a86af744ccfbba7
DRMEncryptedSecretKey.bin	521906dacc570cc89b784af8a782cb777fc78287f014b533a3eddd3cea8a0483
DRMExpiredBody.txt	91f033be557de1bb7cf8060ecea97be8ee11093c8c00e6d14e1f58371ad51201
DRMExternalBody.txt	dbd3a94058d5ac8ad2fa1341da81ac3e2e9be2b33aad086c0432e7abfbe9feea
hcode.txt	793b2168f98fe148522ced95283c0c80afdfdd373b4e0682b7ddb57f6909a3f6
readme.txt	ce5285c647989ef60a86688ad4bdf61d2590c0518a0aac0479c6db1dc83ca4b2
saconfig.ini	29a1387f7f371545b62a40b048272e60f67cbf8fd8aebfa3ee79c9c734bbad76
sage8017.exe	44b701a01b8759dc4450ce1f276a819e6daa2a795a532c648586a43932a8f180
sage_ca2cert.der	fe6103c05f95f61acf3aa3dabfab34024246527c6d5b2b2c66e7078941b5d12f
SecureAge Admin Guide.pdf	f0c48759c7f84b3c9f4ff1f67032a47c06573c14d930aa30f368d1ba93854a4b
SecureAge Installation Guide.pdf	80a379ffa273276938aeda9dfa32af72b3ff335c3dd9ab6a2279abcc90664c76
SecureDataCfg64.exe	ab6439df5c6fe40831694bbe6a3f8a6f3e73c5c439349bcf26e702d7c12cc43f
SecurePDFExternalBody.txt	5ecc768cec1f9c4db519c38ce317fd42db9b8c9a117f1c377629ccb3c3cd295b
SecurePDFExternalBodyWithURL.txt	5df1844ed175921c1be1b6783c1c9fca831e931d9da5130d543ffe3c4422b3f9

SecurePDFPswdServCfg.json	a91009c6ad0b450eb26773a7b8aa01ba6ee55ebd39cf51064cfca4e776e29551
setup64.exe	8608570120dc127ef41ce1efa54cd487e90d753dc77ef147a1c0ddd15758d0cb

2. TOE guidance documents in .pdf format provided together with the installation package or via email

Name	Version	Method of delivery
SecureAge 8.0 Administrator Guide	Jan 2022	CD or download link (included in installation package)
SecureAge 8.0 Installation Guide	Sep 2021	CD or download link (included in installation package)
SecureAge 8.0 User Guide	Jun 2022	CD or download link (included in installation package)
SecureAge 8.0 Uninstallation Guide	Jun 2021	CD or download link (included in installation package)
SecureData 8.0 Operational User Guidance and Preparative Procedures Supplement	0.8	Email

3. SecureData activation license key provided via email

- Software file, which will be extracted after Suite package has been successfully installed:
  - Windows\System32\drivers\SecureData.sys
  - Windows\System32\drivers\SdsPscA.sys
  - Windows\System32\drivers\SdsPscB.sys
  - Windows\System32\drivers\SdsPscC.sys
  - Windows\SdsCfg.dat
- User Guidance documents, which are in pdf format, are included in SecureAge software, except Operational User Guidance and Preparative Procedure Supplement. "SecureAge 8.0 Operational User Guide and Preparative Procedures Supplement" can be sent via email upon customer request. The following are the list of user guidance documents:
  - SecureAge 8.0 Administrator Guide, Jan 2022
  - SecureAge 8.0 Installation Guide, Sep 2021
  - SecureAge 8.0 User Guide, Jun 2022
  - SecureAge 8.0 Uninstallation Guide, Jun 2021
  - SecureData 8.0 Operational User Guidance and Preparative Procedures Supplement, Ver 0.8

1.6.3 Logical scope of the TOE

The following is the list of TOE logical scope that defined in this document, covers by the Security Functional Requirements (SFRs).

A. File Encryption. TOE provides the capability in performing file encryption and decryption. Below describes this process after user successfully login SecureAge profile.

Create Encrypted File: prepare necessary information for TOE operation.

Read Encrypted File: decrypt the file content with the correct AES key.

Write Encrypted File: encrypt the file content with the correct AES key.

B. Fault Tolerance. TOE has the capability in operate during failure in which the TOE operations in secure state if there were a power failure or physical anomaly inflicting temporary failure of disk operation during the process of TOE background encryption. If there were a failure of TOE operations, this only will be affecting the temporary file(s), and not the original file.

1.7 Evaluated Configuration

The following installation and configuration options must be used:

1. Computer used to install TOE need to enable Secure Boot.
2. TOE user will login Windows OS with a non-system administrator role.
3. Prior to installation, the administrator can perform modification on the TOE policy via Configuration tool. It is noted that the Organization security policy shall be configured to allow only administrator to install the TOE.
4. User with administrator privilege can configure the TOE policy through TOE Policy Configuration file (SecureDataCfg64.exe), under SecureData Options, set below fields to 'No':
    - CopyInPlainTo
    - CopyInPlain
    - ManualDecrypt
5. The TOE policy changes only take place upon installation / reinstallation of the TOE. User will only use reliable PKI system to generate SecureAge user profile digital ID, such as build-in SecureAge CA.
6. In SecureAge's configuration file, autoconf.ini under TOE installation folder, set field of 'Link To Windows Login' value to 0. This will disable 'Link to Windows Login' feature.

2 CONFORMANCE CLAIM

The ST and TOE are conformant to version 3.1 (REV 5) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 5), April 2017, extended by security functional component as defined in Section 5.
- **Part 3 conformant, EAL2+.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 5), April 2017. The Evaluation is EAL2 augmented with ALC_FLR.2.
- No conformance to a Protection Profile is claimed.

3 SECURITY PROBLEM DEFINITION

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The TOE addresses the following threats.

Table 3: TOE Threats

Identifier	Threat statement
T.INFO_LEAK	An attacker may get original file content without having permission from the TOE user (in which the person who owns, or is responsible for, the information). It will happen when the device got stolen or falls into the hands of an attacker.
T.WEAK_CRYPTO	An attacker may successfully decrypt the encrypted data if weak or out of date cryptography method has been used.

3.3 Organisational security policies

Identifier	OSP statement
OSP.Windows	Organization should ensure that the IT security policy only allows only administrator to install the TOE.

3.4 Assumptions

The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 4: TOE Assumptions

Identifier	Assumption statement
A.AUTHORIZED_USER	TOE user is trusted, not hostile and well trained with information security awareness, such as prevent any social engineering attacks, understood the importance of keeping information of data/files plus password and TOE user private/public keys in private (securely).
A.NOEVIL	Administrator responsible for configuring, installing and remove the TOE is assumed not hostile and is competent.
A.EVALUATION_CONFIG_KEYS_CERT	When administrator uses a third-party PKI support system for key generation (PKCS#11 compliance smart cards or tokens or HSM or password protected software keys), it is assumed that the managing of keys and certificates will be fully responsible by the third-party PKI system to ensure the keys generated are not malicious to the TOE operation.
A.OS	TOE should be installed in a secure and malware-free operating system.

4 SECURITY OBJECTIVES

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. They are security objectives for the TOE to address and additional objectives that provide specific direction for the intended environment in which the TOE is to operate.

4.2 Security Objectives for the TOE

Table 5: Security Objective for the TOE

Identifier	Objective statements
O.CRYPTO_OP	The TSF shall enforce AES cryptographic operation managed by the TOE in protecting the data/file(s) and encryption keys.
O.ENCRYPT_DATA	The TSF will provide the means of protecting the confidentiality of user data file stored on the system hard disk drives and enforce all files and folders copy to external drives (removable drives or network drives) will be encrypted. And TSF will protect the original when background encryption is conducted.

4.3 Security Objectives for the TOE Operational Environment

Table 6: Security Objective for the TOE Operational Environment

Identifier	Objective statements
OE.OPERATIONAL_GUIDANCE	Administrator must ensure that the TOE is delivered, installed, configured, administered and operated in a manner that were advised by the TOE Developer to maintains its integrity, include providing a secure and malware-free operating system.
OE.USER_GUIDANCE	TOE user should be provided documentation containing sufficient information to guide in operating the TOE.
OE.THIRD_PARTY_PKI_SYSTEM	Administrator must ensure that only trusted third-party PKI system will be used to generate TOE user digital ID.
OE.NO_EVIL	Administrator should be adequately trained, responsible and honest individuals who are not motivated to disable, degrade or subvert the operation of the TOE in the environment for personal gain or other purposes that contradict the security policies of the organization.

Identifier	Objective statements
OE.SEC_AWARE	TOE user and administrator should be properly trained in organizational security policy and have awareness of security procedures. Thus, TOE user should not share their password and abide to the rules and regulations of the organization when using the TOE.
OE.Windows	Windows security policy of the organization should be configured to allow only administrator to be able to install the TOE.

4.4 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions and threats.

Table 7: Security Objective Rational Mapping

THREATS/ ASSUMPTIONS/ OSP / OBJECTIVES	T.INFO_LEAK	T.WEAK_CRYPTO	A.AUTHORISED_USER	A.NOEVIL	A.EVALUATION_CONFIG_KEYS_CERT	A.OS	OSP.Windows
O.CRYPTO_OP		☒					
O.ENCRYPT_DATA	☒						
OE.OPERATIONAL_GUIDANCE				☒		☒	
OE.USER_GUIDANCE			☒				
OE.THIRD_PARTY_PKI_SYSTEM					☒		
OE.NO_EVIL				☒			
OE.SEC_AWARE			☒	☒			
OE.Windows							☒

4.4.1 TOE Security objectives rationale

The following table demonstrates that all security objectives for the TOE are trace back to the threats in the security problem definition.

Table 8: Security Objective Rationale Justification

Threats	Objectives	Rationale
T.INFO_LEAK	O.ENCRYPT_DATA	This threat is mitigated because: O.ENCRYPT_DATA ensure that the file, both in transit and at rest, is protected by encryption.
T.WEAK_CRYPTO	O.CRYPTO_OP	The threat of weak cryptographic methods that provide insufficient security is mitigated by implementing approved cryptographic methods.

4.4.2 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment are trace back to assumptions in the security problem definition.

Table 9: Environment Security Objective Rationale Justification

Assumptions	Objective	Rationale
A.AUTHORIZED_ USER	OE.USER_GUIDANCE OE.SEC_AWARE	OE.USER_GUIDANCE and OE.SEC_AWARE address the assumption A.AUTHORIZED_USER by providing the sufficient guidance and training to the TOE users to use the TOE correctly and securely.
A.NOEVIL	OE.OPERATIONAL_ GUIDANCE OE.SEC_AWARE OE.NO_EVIL	OE.OPERATIONAL_GUIDANCE, OE.SEC_AWARE and OE.NO_EVIL address the assumption A.NOEVIL by ensuring that administrator have sufficient training and guidance to competently configure the TOE before TOE installation in order to maintain the security of the TOE.
A.EVALUATION_CON FIG_KEYS_CERT	OE.THIRD_PARTY_PKI_ SYSTEM	OE.THIRD_PARTY_PKI_SYSTEM addresses this assumption by ensuring that TOE user digital ID is generated from trusted third-party PKI system.

Assumptions	Objective	Rationale
A.OS	OE.OPERATIONAL_ GUIDANCE	OE.OPERATIONAL_GUIDANCE address this assumption by ensuring that administrator will provide a secure and malware-free operating system.
OSP.Windows	OE.Windows	OE.Windows enforces the OSP by requiring the Windows security policy to be configured to allow only administrator to be able to install the TOE.

5 EXTENDED COMPONENTS DEFINITION

No extended components have been defined for this ST.

6 SECURITY REQUIREMENTS

6.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].
- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].
- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.
- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

6.2 Security functional requirements

6.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 6.1 above and are itemised in the table below.

Table 10: SFRs

Identifier	Title
Cryptographic Support	
FCS_COP.1	Cryptographic operation
FCS_CKM.1	Cryptographic Key Generation
FCS_CKM.4	Cryptographic Key Destruction
Fault Tolerance	
FPT_FLS.1	Failure with preservation of secure state

Identifier	Title
FRU_FLT.1	Degraded fault tolerance

6.2.2 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in XTS mode**] and cryptographic key sizes [**256 bits**] that meet the following: [**FIPS 197/ and SP 800-38E**].
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.4 Cryptographic key destruction
Notes:	TOE Build-in SecureAge Crypto is a collection of cryptographic functions that implement FIPS approved algorithm, details are shown as below: https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/details?validation=34484&displayMode=CollapsedAlgorithm This is refer to Session Key encryption and file content encryption.

6.2.3 FCS_CKM.1 Cryptographic key generation

Hierarchical to:	No other components.
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**SHA256 Hash DRBG**] and specified cryptographic key sizes [**256 bits**] that meet the following: [**NIST SP 800-90A Rev. 1**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	This refers to Session Key generation for file content encryption.

6.2.4 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**zeroization**] that meets the following: [**none**].
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]
Notes:	This refers to plain Session Key destruction after file operation complete and AES key destruction after logout Suite.

6.2.5 FPT_FLS.1 Failure with preservation of secure state

Hierarchical to:	No other components.
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: [**power failure or physical anomaly inflicting temporary failure of disk operations during encryption / decryption of files**].
Dependencies:	No dependencies.
Notes:	None.

6.2.6 FRU_FLT.1 Degraded fault tolerance

Hierarchical to:	No other components.
FRU_FLT.1.1	The TSF shall ensure the operation of [**background encryption files and folders on local drives**] when the following failures occur: [**power failure or physical anomaly inflicting temporary failure of disk operation during background encryption**].
Dependencies:	FPT_FLS.1 Failure with preservation of secure state
Notes:	Background encryption refers to operation of file sharing, initial background encryption after TOE successful installation and manual encryption.

6.3 TOE Security assurance requirements

EAL2 requires evidence relating to the design information and test results but does not demand more effort on the part of the developer than is consistent with good commercial practice.

EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description on the architecture of the TOE, to understand the security behaviours.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to attackers with basic attack potential.

EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Table 11: SARs

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage

Assurance class	Assurance components
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
	ALC_FLR.2 Flaw Remediation
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
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

6.4 Security requirements rationale

6.4.1 Dependency rationale

The table below demonstrates the mutual supportiveness of the SFRs for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level of EAL2, as defined in the Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

Table 12: SFRs Justification

SFR	Dependency	Inclusion
FCS_COP.1	[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.4 Cryptographic key destruction	FCS_CKM.1 FCS_CKM.4
FCS_CKM.1	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1 FCS_CKM.4
FCS_CKM.4	[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.1
FPT_FLS.1	No dependencies.	N/A
FRU_FLT.1	FPT_FLS.1 Failure with preservation of secure state	FPT_FLS.1

1 – justification for not include FMT_MSA.3: The file content access method is part of TOE design and it is not configurable.

6.4.2 Mapping of SFRs to security objectives for the TOE

Table 13: SFRs Mapping to Security Objectives

Security objective	Mapped SFRs	Rationale
O.CRYPTO_OP	FCS_COP.1	FCS_COP.1 state that AES is used for data encryption and decryption.
	FCS_CKM.1	FCS_CKM.1 state that cryptographic keys and parameters are generated with standards-based algorithms.
	FCS_CKM.4	FCS_CKM.4 states that the cryptographic keys and parameters are safely destroyed when their lifetime ends or when the TOE user forces generation of new keys. Keys are zeroized in accordance with FIPS 140-2 specifications

Security objective	Mapped SFRs	Rationale
O.ENCRYPT_DATA	FCS_COP.1	FCS_COP.1 states that AES is used for data encryption and decryption. This ensures that all data files are protected.
	FPT_FLS.1	FPT_FLS.1 provides the TOE will preserve a secure state in the event of power failure or physical anomaly inflicting temporary failure of disk operations during encryption / decryption of files.
	FRU_FLT.1	FRU_FLT.1 ensures the operation of background encryption files and folders on local drives when power failure or physical anomaly inflicting temporary failure of disk operation during background encryption.

6.4.3 Explanation for selecting the SARs

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2) with augmented of ALC_FLR.2.

The TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

7 TOE SUMMARY SPECIFICATION

7.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE actually implements the claimed security functional requirements.

The TOE security functions include the following:

- File Encryption
- Fault Tolerance

7.2 File encryption

TOE performs the following cryptographic operations for all read / write file operations on local drives or removable drives or network drives. TOE encryption is based on the AES in XTS mode algorithm with each data file protected by a different randomly generated 256-bits AES Session Key. Hash DRBG (256 bits) algorithm is used to generate cryptographic keys (Session Keys).

Note that, in the event of any revocation of keys used by the TOE user or creating a new Session Key, the previous key will be remove using zeroization process.

When the TOE user tries to create the new data file on local drives or removable drives or network drives, TOE generates AES 256 bits random Session Key, and the data blocks are tweaked with the file offset and the generated Session Key. The tweaked data contents are encrypted with the Session Key (AES in XTS mode).

When the TOE user tries to read the encrypted file on local drives or removable drives or network drives, they need to use the correct Session Key to decrypt the file content, the decrypted data blocks are tweaked with the file offset and the Session Key to get the original data blocks.

When the TOE user tries to update the data contents in the encrypted file, TOE tweaks the data contents with the file offset and the decrypted Session Key which was in the memory, encrypts the data contents with the Session Key (AES in XTS mode) and writes the encrypted data contents back to the file.

When TOE users encrypt / re-encrypt the files manually, the TOE will encrypt / re-encrypt the files depends on the encryption options (i.e., ‘Encrypt Plain Files’ or ‘Re-encrypt User’s Encrypted Files’ or ‘Re-encrypt Other’s Encrypted Files’, etc.) set by the TOE user.

Security Functional Requirements: FCS_COP.1, FCS_CKM.1, FCS_CKM.4

7.3 Fault tolerance

After successful installation of TOE and the system is rebooted, the initial background encryption will be run once to make sure all TOE user data/file(s) and folders will be encrypted based on pre-defined policies. During the background encryption process, the encryption TSF will encrypt the file in such a way that it encrypts the file in the temporary file and then it replaces the original file with the encrypted temporary file with the same original file name.

In addition, operation of file sharing and manual encryption also consider as background encryption and same process as initial background encryption will apply.

If there is a power failure or physical anomaly inflicting temporary failure of disk operation during the background encryption, only the temporary file which is currently processing will be corrupted. The chances of failure occurred during replacing process are very low and there are third party software in the market to recovery this type of failure. TOE maintains the failed secure state of the user data files on local drives during background encryption.

Security Functional Requirement: FPT_FLS.1, FRU_FLT.1

8 REFERENCE

NIST SP 800-90A Rev. 1	National Institute of Standards and Technology Special Publication 800-90A Revision 1 - Recommendation for Random Number Generation Using Deterministic Random Bit Generators
FIPS 197	Federal Information Processing Standards Publication 197 - Announcing the Advanced Encryption Standard (AES)
NIST SP 800-132	NIST Special Publication 800-132 - Recommendation for Password-Based Key Derivation Part 1: Storage Applications
NIST SP 800-38E	Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices