Certificate Report

Version 1.0

19 September 2023

CCA_CC_20004

For

SecureData version 8.0

From

SecureAge Technology Pte Ltd

This page is left blank intentionally

Foreword

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

https://www.commoncriteriaportal.org

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

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

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

This certification is not an endorsement of the product.

Amendment Record

Version	Date	Changes
0.1	21 August 2023	Draft
1.0	19 September 2023	Released

NOTICE

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

Executive Summary

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

The Target of Evaluation (TOE) is the SecureData, version 8.0 and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Identifier	Version
Software	Windows\System32\drivers\SecureData.sys
	Windows\System32\drivers\SdsPscA.sys
	Windows\System32\drivers\SdsPscB.sys
	Windows\System32\drivers\SdsPscC.sys
	Windows\SdsCfg.dat

Table 1 - TOE components identifier

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

Name	Version	Method of Delivery
SecureAge 8.0 Administrator Guide	Jan 2022	CD or download link
SecureAge 8.0 Installation Guide	Sep 2021	CD or download link
SecureAge 8.0 User Guide	Jun 2022	CD or download link
SecureAge 8.0 Uninstallation Guide	Jun 2021	CD or download link
SecureData 8.0 Operational User Guidance and Preparative Procedures Supplement	Ver 0.8, 26 Jun 2023	PDF by Email

Table 2 - List of guidance documents

SecureData is one of the tools within the SecureAge Security Suite (Suite), providing the user endpoint with automatic file and folder encryption for seamless security of all user files. 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 four components (SecureData, SecureFile, SecureDisk, and SecureEmail) and each component can be activated individually by providing valid license code.

The main 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 if the 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 can decrypt the data/file(s).

There are two types of TOE usage:

I. Normal file operation: the TOE is designed and registered as one of Windows OS system driver, each time when user conducts the operation, such as read, write, or 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.

II. Background encryption: this refers to operation of file sharing, initial background encryption after successful TOE installation and manual encryption. Different from normal file operation, user needs to invoke TOE via right click menu in Windows (initial background encryption is automatically triggered after the user's 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, thus protecting the original file.

The evaluation of the TOE has been carried out by UL Verification Services Pte Ltd, an approved CC test laboratory, at the assurance level CC EAL 2 augmented with ALC_FLR.2 and completed on 14 September 2023.

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

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

TOE Security Functionality
File Encryption TOE provides the capability in performing file encryption and decryption. - Create Encrypted File - Read Encrypted File - Write Encrypted File **Security Functional Requirements:** FCS_COP.1, FCS_CKM.1, FCS_CKM.4
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. **Security Functional Requirements**: FPT_FLS.1, FRU_FLT.1

Table 3: TOE Security Functionalities

Please refer to the Security Target [1] for more information.

The assets to be protected by the TOE has been defined. Based on these assets, the TOE Security Problem Definition has been defined in terms of Assumptions, Threats and Organisation Policies. These are outlined in Chapter 3 of the Security Target [1]

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

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate applies only to the specific version and release of the IT product in its evaluated configuration. This certificate is not an endorsement of the IT product by SCCS, and no warranty of the IT product by SCCS, is either expressed or implied.

Table of Contents

1 Certification

1.1 Procedure

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

- Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [2] [3] [4];
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 5 [5]; and
- SCCS scheme publications [6] [7] [8]

1.2 Recognition Agreements

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

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

2 Validity of the Certification Result

This Certification Report only applies to the version of the TOE as indicated. The Certificate is valid till **19 September 2028**[1].

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

The owner of the Certificate is obliged:

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

[1] Certificate validity could be extended by means of assurance continuity. Certificate could also be revoked under the conditions specified in SCCS Publication 3 [8]. Potential users should check the SCCS website (https://www.csa.gov.sg/our-programmes/certification-and-labelling-schemes/singapore-common-criteria-scheme/product-list) for the up-to-date status regarding the certificate's validity.

3 Identification

The Target of Evaluation (TOE) is: SecureData version 8.0.
The physical deliverable of the TOE comprised of the following items:

TOE software installation file (SecureAge Security Suite installation package) delivered to the customer in the form of CD or unique download link.

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

Table 4 - TOE Deliverables

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

Name	Version	Method of Delivery
SecureAge 8.0 Administrator Guide	Jan 2022	CD or download link
SecureAge 8.0 Installation Guide	Sep 2021	CD or download link

SecureAge 8.0 User Guide	Jun 2022	CD or download link
SecureAge 8.0 Uninstallation Guide	Jun 2021	CD or download link
SecureData 8.0 Operational User Guidance and Preparative Procedures Supplement	Ver 0.8, 26 Jun 2023	PDF by Email

Table 5 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	SecureData 8.0
Security Target	SecureData 8.0 Security Target
Developer	SecureAge Technology Pte Ltd
Sponsor	SecureAge Technology Pte Ltd
Evaluation Facility	UL Verification Services Pte Ltd
Completion Date of Evaluation	14 September 2023
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_20004
Certificate Validity	5 years from date of issuance

Table 6: Additional Identification Information

4 Security Policy

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

The TOE implements policies pertaining to the following security functional classes:

- Cryptographic Support
- Fault Tolerance

Specific details concerning the above-mentioned security policy can be found in Chapter 6 of the Security Target [1].

5 Assumptions and Scope of Evaluation

5.1 Assumptions

The assumptions defined in the Security Target [1] and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE environment and are listed in the tables below:

Environmental Assumptions	Description
OE.OPERATIONAL_GUIDANCE	TOE 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	TOE administrator must ensure that only trusted third-party PKI system will be used to generate TOE user digital ID.
OE.NO_EVIL	TOE administrator roles 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.
OE.SEC_AWARE	TOE user and TOE 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.

Table 7: Environmental Assumptions

Details can be found in section 4.3 of the Security Target [1].

5.2 Clarification of Scope

The scope of evaluation is limited to the claims made in the Security Target [1].

Users are reminded to set up the TOE as per guidance. Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

5.3 Evaluated Configuration

SecureData is one of the tools of SecureAge Security Suite (Suite), providing the user endpoint with automatic file and folder encryption for security of all user files. 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 four components (SecureData, SecureFile, SecureDisk, and SecureEmail) and each component can be activated individually by providing valid license code.

The main 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 If the 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 authorised 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:

I. 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.

II. Background encryption: this refers to operation of file sharing, initial background encryption after successful TOE installation and manual encryption. Different from normal file operation, user needs to invoke TOE via right click menu in Windows (initial background encryption is automatic triggered after user’s 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.

5.4 Non-Evaluated Functionalities

There are no non-evaluated functionalities within the scope as clarified in section 5.2.

5.5 Non-TOE Components

The TOE requires the following non-TOE components for its operation.

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 four separate components (SecureData, SecureFile, SecureDisk and SecureEmail), SecureAge Security Suite provides 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 pair generation • User Key generation Refer to Section "Evaluated Configuration" below for any specific setup requirement for Suite.

Table 8: Minimum System Requirements

Evaluated Configuration:

The following installation and configuration options must be used:

i. Computer used to install TOE needs to enable Secure Boot.

ii. TOE user will login to Windows OS with a non-system administrator role.

iii. Prior to installation, the administrator can perform modification on the TOE policy via Configuration tool. It is noted that the Organisation Security Policy shall be configured to allow only administrator to install the TOE

iv. User with administrator privilege can configure the TOE policy through the TOE Policy Configuration file (SecureDataCfg64.exe), under SecureData Options, set below fields to 'No':

   a. CopyInPlainTo
   b. CopyInPlain
   c. ManualDecrypt

v. 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.

vi. In SecureAge's configuration file, autoconf.ini under TOE installation folder, set field of 'Link To Windows Login' value to zero. This will disable 'Link to Windows Login' feature.

6 Architecture Design Information

TOE design is analysed in detail in Single Evaluation Report (SER) – ADV Class. A brief overview is presented in this section. In order to provide above security functions, there are 3 subsystems designed within TOE as below:

- Configuration Management subsystem: responsible for the management of TOE security features;
- System Control subsystem: fault tolerance; and
- File Encryption subsystem: responsible for cryptographic operations during read / write file.

The subsystems of the TOE and the TSF role of each subsystem is summarized in the table below:

Subsystem	TSF Subsystem	Category	Interaction with	Evaluator Notes
System Control	Yes	SFR-enforcing	File Encryption	This subsystem provides fault tolerance function.
File Encryption	Yes	SFR-enforcing	System Control	This subsystem provides file encryption function during file operation.

Table 9: Analysis of TOE subsystems

The logical architecture of the TOE in its operational environment is shown in the figure below:

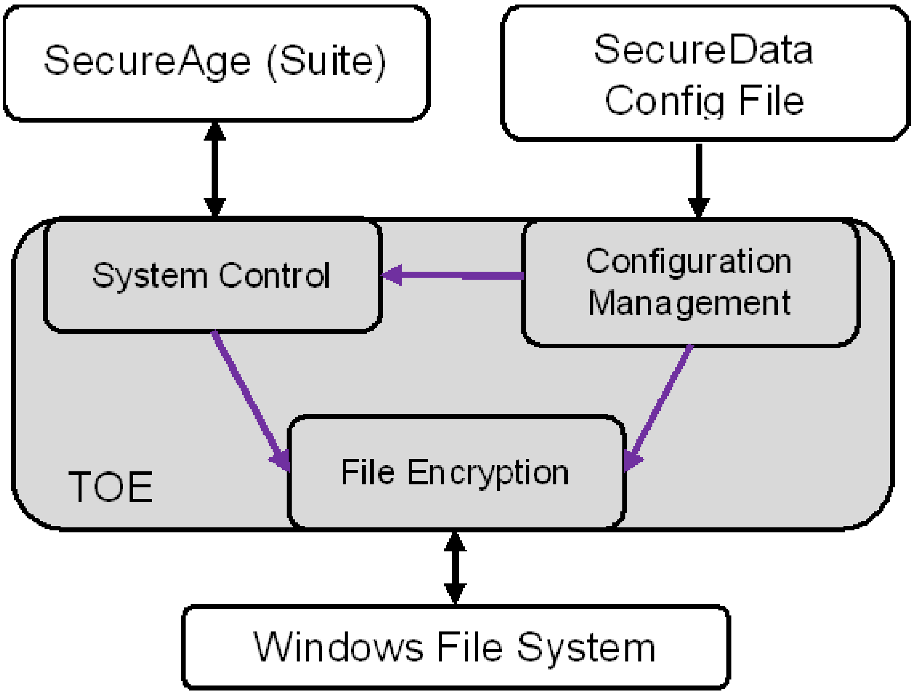

Figure 1 TOE subsystem logical architecture

SecureData Driver is registered as one of Windows OS File System Drivers. Every time user conducts a file operation within Windows OS, TOE will be invoked via this Windows Operating System interface to complete the process by performing encryption/decryption of the file content. In order to get the user key from SecureAge Security Suite, TOE communicate with the suite vis SecureData System Control interface. And each time when update the TOE configuration, TOE will load the latest configuration via SecureData config file interface.

7 Documentation

The evaluated documentation as listed in

Name	Version	Method of Delivery
SecureAge 8.0 Administrator Guide	Jan 2022	CD or download link
SecureAge 8.0 Installation Guide	Sep 2021	CD or download link
SecureAge 8.0 User Guide	Jun 2022	CD or download link
SecureAge 8.0 Uninstallation Guide	Jun 2021	CD or download link
SecureData 8.0 Operational User Guidance and Preparative Procedures Supplement	Ver 0.8, 26 Jun 2023	PDF by Email

Table 5 - Guidance Document (part of TOE deliverables)

is being provided with the product to the customer. These documentations contain the required information for secure usage of the TOE in accordance with the Security Target.

8 IT Product Testing

8.1 Developer Testing (ATE_FUN)

8.1.1 Test Approach and Depth

The evaluator sampled and repeated the developer's testing to validate the correctness of the TSF at the TSFI and the subsystem level.

8.1.2 Test Configuration

The TOE used for testing is configured according to the TOE guidance document [9] [10] [11] [12] [13].

8.1.3 Test Results

The test results provided by the developer covered all operational functions as described in the Security Target [1].

All test results from all tested environment showed that the expected test results are identical to the actual test results.

8.2 Evaluator Testing (ATE_IND)

8.2.1 Test Approach and Depth

The evaluator devised a test subset sampling and repeating developer’s tests and included additional test cases:

- To make sure that the tests cover all the SFR-enforcing TSFIs.
- To make sure that the TSF is operate as per functional specification described.

8.2.2 Test Configuration

A detailed test description was provided in the ATE document. The evaluator set up their own test environment following the developer’s guidance documents Prior to running tests, the evaluator performed identification of the test environment and verification of the TOE.

8.2.3 Test Results

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

8.3 Penetration Testing (AVA_VAN)

8.3.1 Test Approach and Depth

The evaluator conducted a vulnerability search online using public sources of information, including National Vulnerability Database (NVD by NIST), cve.org and exploit-db.com etc. The following search term were used:

Search Terms

- SecureAge exploit
- SecureAge vulnerability
- SecureAge CVE
- SecureData exploit
- SecureData vulnerability
- SecureData CVE
- Encryption software exploit
- Encryption software vulnerability

Combined with the analysis of the TOE, the evaluator then identified potential vulnerabilities applicable to the TOE in its operational environment. Attack scenarios were then devised and a theoretical analysis of the attack potentials for the scenarios were performed. Penetration tests were conducted for scenarios where the attack potentials were Basic.

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

Penetration Test	Description
Test 1 – Process memory disclosure in SecureAge authentication process	This test is to ensure that sensitive information such as SecureAge Profile's Password and Private Key that used during authentication are not being cached in cleartext inside of process memory.
Test 2 – Hardcoded strings in SecureAge binaries	This test is to ensure no hardcoded sensitive strings in the binaries that will leak useful information to attackers.
Test 3 – Sensitive information in kernel memory dump	This test is supplement of test 1, which is focus on kernel memory dump file. This test is used to verify that sensitive information, such as SecureAge Profile's Password, User Key and mask, that are being used not retrievable from kernel memory dump.
Test 4 – Underlying OS registry analysing	This test is used to assess if any sensitive information such as system keys and user keys stored in registry.
Test 5 – System file analysis for hash values	This test is supplement of test 2, which is focus on TOE system files' hash values. This test case is to check if the hash values that being saved in system file can be found.
Test 6 – Hardcoded strings in SecureData driver	This test is supplement test 2, which is to test SecureData driver file. This test is to ensure no hardcoded sensitive strings in the driver file that will leak useful information to attackers.

Table 10 - Penetration Test Case

Vulnerabilities discovered during the penetration testing have been resolved.

9 Results of the Evaluation

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

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

This implies that the TOE satisfies the security requirements specified in the Security Target [1].

10 Obligations and recommendations for the usage of the TOE

The documents as outlined in Table 2 - List of guidance documents contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition, all aspects of Assumptions, Threats and OSPs as outlined in the Security Target [1] that are not covered by the TOE shall be fulfilled by the operational environment of the TOE.

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

Users are reminded to set up the TOE as per guidance documents to correctly deploy and use the TOE in the evaluated configuration.

The following is provided by the evaluator to highlight features and requirements that are critical to the secure operation of the TOE. This is by no means an exhaustive list of the documents to securely use the TOE. Refer to product guidance documentation for a complete pre-operation and user guidance.

TOE is running on Windows Operating System, therefore maintain OS security is important for TOE to maintain secure operation. TOE user will need to consider hardening the OS based on well-known guide, such as Microsoft recommendation or CIS Benchmarks. The Windows security policy of the organisation will need to be configured to allow only the administrator to install the TOE.

TOE will conduct background encryption immediately and automatically after the user profile has been created. Without proper setup, it might result in OS not working properly, therefore it is strongly recommended to have qualified administrator to conduct the whole TOE setup, configuration and verify it is working before releasing to end user.

As TOE design is focus on protecting data confidentiality, TOE user is strongly advised to backup critical data and ensure the data can be retrieved when needed.

User key pair is the only key to decrypt the encrypted data, TOE user is strongly advised to protect it.

11 Acronyms

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

12 Bibliography

[1] SecureAge Technology Pte Ltd, “SecureData 8.0 Security Target, Version 1.0,” 12 April 2023.

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

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

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

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

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

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

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

[9] SecureAge Technology Pte Ltd, “SecureAge 8.0 Administrator Guide Based on SecureAge Version 8.0,” January 2022.

[10] SecureAge Technology Pte Ltd, “SecureAge 8.0 Installation Guide Based on SecureAge Version 8.0,” September 2021.

[11] SecureAge Technology Ptd Ltd, “SecureAge 8.0 User Guide Based on SecureAge Version 8.0,” June 2022.

[12] SecureAge Technology Pte Ltd, “SecureAge 8.0 Uninstallation Guide Based on SecureAge Version 8.0,” June 2021.

[13] SecureAge Technology Pte Ltd, “SecureAge 8.0 Operational User Guidance and Preparative Procedures Supplement, Version 0.8,” 26 June 2023.

---End of Report --