Certificate Report

Version 1.0

9 October 2023

CSA_CC_22004

For

SG-KMS, version 1.0.0012-GA

From

PT Sandhiguna Widya Proteksi

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	17 August 2023	Draft
1.0	9 October 2023	Released

NOTICE

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

Executive Summary

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

The Target of Evaluation (TOE) is the SG_KMS, version 1.0.0012-GA and has undergone the CC certification procedure at the Singapore Common Criteria Scheme (SCCS). The TOE comprises of the following components:

Identifier	Version
Software	SGKMS Centralized Cryptographic Engine and Vault (CCEV) File name: sgkms-ccev-1.0.0012. el8.x86_64.rpm Format: rpm file Delivery method: Email with PGP protection
	SGKMS Local Cryptographic Engine and Vault (LCEV) File name: sgkms-lcev-1.0.0012. el8.x86_64.rpm Format: rpm file Delivery method: Email with PGP protection

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
System Administrator Guide	v1.0.0012-GA	Email with PGP protection
Deployment Guide	v1.0.0012-GA	Email with PGP protection
SGCLI Deployment Guide	v1.0.0012-GA	Email with PGP protection
SGKMS Rest API	v1.0.0012_GA	Email with PGP protection

Table 2 - List of guidance documents

The TOE, namely, SG-KMS, is a software that provides cryptographic services and key management services to secure data. The clients deploy the TOE to generate and manage their cryptographic keys, certificates, secrets, attributes, and metadata.

SG-KMS as the TOE provides separate modules for cryptographic services and key management services. The module that handles key management services is called centralized cryptographic engine and vault (CCEV) whereas the module that provides cryptographic services is called local cryptographic engine and vault (LCEV). Depending on the specific needs of the client, SG-KMS allows for the setup of either a single LCEV or several distributed LCEVs.

TOE consists of the following logical scope:

- Cryptographic Support
- User Data Protection

- Identification and Authentication
- Security Management
- TSF Protection
- TOE Access
- Trusted Path
- Resource Utilisation
- Security Audit

The evaluation of the TOE has been carried out by An Security Pte Ltd, an approved CC test laboratory, at the assurance level CC EAL 2 augmented with ALC_FLR.1 (Flaw Remediation) and completed on 2 October 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
Cryptographic Support The TOE provides two main services, namely, key management services and cryptographic services. The TOE is capable to perform the following cryptographic operations: symmetric encryption and decryption using AES, asymmetric encryption and decryption using RSA and ECDSA, digital signature generation and verification using RSA and ECDSA, cryptographic hashing using SHA-2, message authentication using HMAC, CMAC, and GMAC, Key Agreement Scheme using ECC, key derivation function using PBKDF2, key destruction using zeroization, key distribution using DHE and ECDHE, and secret sharing scheme using Shamir Secret Sharing. In support of these operations, the objects are managed by key management services. The components of the TOE are connected to each other via cryptographic protocols, i.e., mTLS.
User Data Protection User data is only distributed among clients' applications and LCEVs. Communication between them is protected by mTLS. To ensure that cryptographic services are provided securely by the LCEVs, the TOE implements an access control policy. The TOE generates security attributes, including keys and slots, in the CCEV. These keys and slots are transmitted to the LCEVs to carry out cryptographic operations. The TOE protects the transmission by creating a secure channel that relies on mTLS.
Identification and Authentication The users of the TOE comprise administrators, agents, and a special agent who access, manage, and configure the TOE. The TOE identifies and authenticates all users before granting them access to the TOE. The TOE identifies users through their identity (IDs) and authenticates them through a password and/or a smart card which stores a private key and certificates. Higher privileged services require more than one administrator to authenticate. The TOE locks a user account after three consecutive failed authentication attempts within a thirty-minute period.
Security Management The TOE implements a privilege-based security management model. Each service has a well-defined privilege that requires certain security attributes for identification and authentication. The privileges fall into five levels, namely emergency, critical, high, normal, and low. The highest level is emergency, which allows the execution of a service that demands the presence of a special agent. This level is used to restore a CCEV's database and to reset administrator passwords in case the quota to do a dual-control approval cannot be met. The administrator and special agent connect to the CCEV to perform key management functions such as key generation, distribution, rotation,

revocation, recovery, expiry, exporting, importing, and disposal.
TSF Protection The TOE provides the capability to consistently interpret security attributes of user data when shared between the TOE and client application/CLI terminal.
TOE access The TOE terminates a user's interactive session based on the session token's lifetime. In addition, an agent session terminates after an hour and the agent needs to refresh the session. Different with the agent, an administrator session terminates after 10 minutes and the administrator need to re-login.
Trusted Path The TOE provides a trusted path between the following entities: • agent and TOE • administrator/special agent and TOE The trusted path is used in the initial authentication and user operations. Such paths are protected by TLS protocol.
Resource Utilization The TOE allows LCEV to operate independently from CCEV, in turn, cryptographic services provided by LCEV shall be maintained even when CCEV is down.
Security Audit The TOE generates and keeps an audit log for administrators’ activities in the CCEV. The log records the date, time, and type of each event, the identity of each relevant administrator relative to the event, and the outcome, either success or failure represented by error codes. The integrity of the audit log is guaranteed by the HMAC on the record of each event. The entire record is stored and managed in the Audit Log Server. Any administrator can export and archive the audit log record.

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 2 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 **9 October 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: SG-KMS Version 1.0.0012-GA.

The following table identifies the TOE deliverables.

Identifier	Version
Software	SGKMS Centralized Cryptographic Engine and Vault (CCEV) File name: sgkms-ccev-1.0.0012. el8.x86_64.rpm Format: rpm file Delivery method: Email with PGP protection
	SGKMS Local Cryptographic Engine and Vault (LCEV) File name: sgkms-lcev-1.0.0012. el8.x86_64.rpm Format: rpm file Delivery method: Email with PGP protection
	SG-CLI File name: sgcli-1.0.0012. el8.x86_64.rpm Format: rpm file Delivery method: Email with PGP protection
	Audit Server File name: sgkms-audit-1.0.0012. el8.x86_64.rpm Format: rpm file Delivery method: Email with PGP protection
Hardware	Smart cards and readers Delivery method: In-house delivery by registered courier

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
System Administrator Guide	v1.0.0012-GA	Email with PGP protection
Deployment Guide	v1.0.0012-GA	Email with PGP protection
SGCLI Deployment Guide	v1.0.0012-GA	Email with PGP protection
SGKMS Rest API	v1.0.0012_GA	Email with PGP protection

Table 5 - Guidance Document (part of TOE deliverables)

Additional identification information relevant to this Certification procedure as follows:

TOE	SG-KMS Version 1.0.0012-GA
Security Target	SG-KMS Security Target Version 1.5
Developer	PT Sandhiguna Widya Proteksi
Sponsor	PT Sandhiguna Widya Proteksi
Evaluation Facility	An Security Pte Ltd
Completion Date of Evaluation	2 October 2023
Certification Body	Cyber Security Agency of Singapore (CSA)
Certificate ID	CSA_CC_220004
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
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- Resource Utilisation
- TOE Access
- Trusted Path/Channels
- Security Audit

Specific details concerning the above-mentioned security policy can be found in Chapter 4 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.COMPET_USERS	TOE users are trusted and competent.
OE.PHYSICAL_ENV	The TOE is deployed in a physically secured environment.
OE.IT_SUPPORT_COMP	The IT supporting components are trusted and secure.
OE.RELIABLE_TIME	A time server shall be deployed to provide reliable timestamp to the TOE.

Table 7: Environmental Assumptions

Details can be found in section 3.2 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

The TOE, SG-KMS, is a software that provides cryptographic services and key management services to secure data. The TOE consists of two main components i.e. Centralized Cryptographic Engine and Vault (CCEV) and Local Cryptographic Engine and Vault (LCEV). CCEV provides key management services, while the LCEV provides cryptographic services. The TOE allows for the setup of either a single LCEV (1) or several distributed LCEVs (2).

The only difference between the two use cases is the number of LCEVs. Both use cases are the same evaluated configuration because of the following reasons:

1. In both use cases, the TOE are deployed in the same operational environment. Hence, the resultant TSFIs, i.e. REST API, mTLS, One-way TLS and SG-CLS, evaluated are the same. To further explain, the evaluated parameters on these TSFIs are the same.

2. The configuration of each instance of LCEV in a several distributed LCEV setup is the same as the configuration of the one instance of LCEV in single LCEV setup.

Hence, the states of the abovementioned (1) and (2) remain the same even when the number of LCEVs increases. Thus, both TOE use cases are the same evaluated configuration.

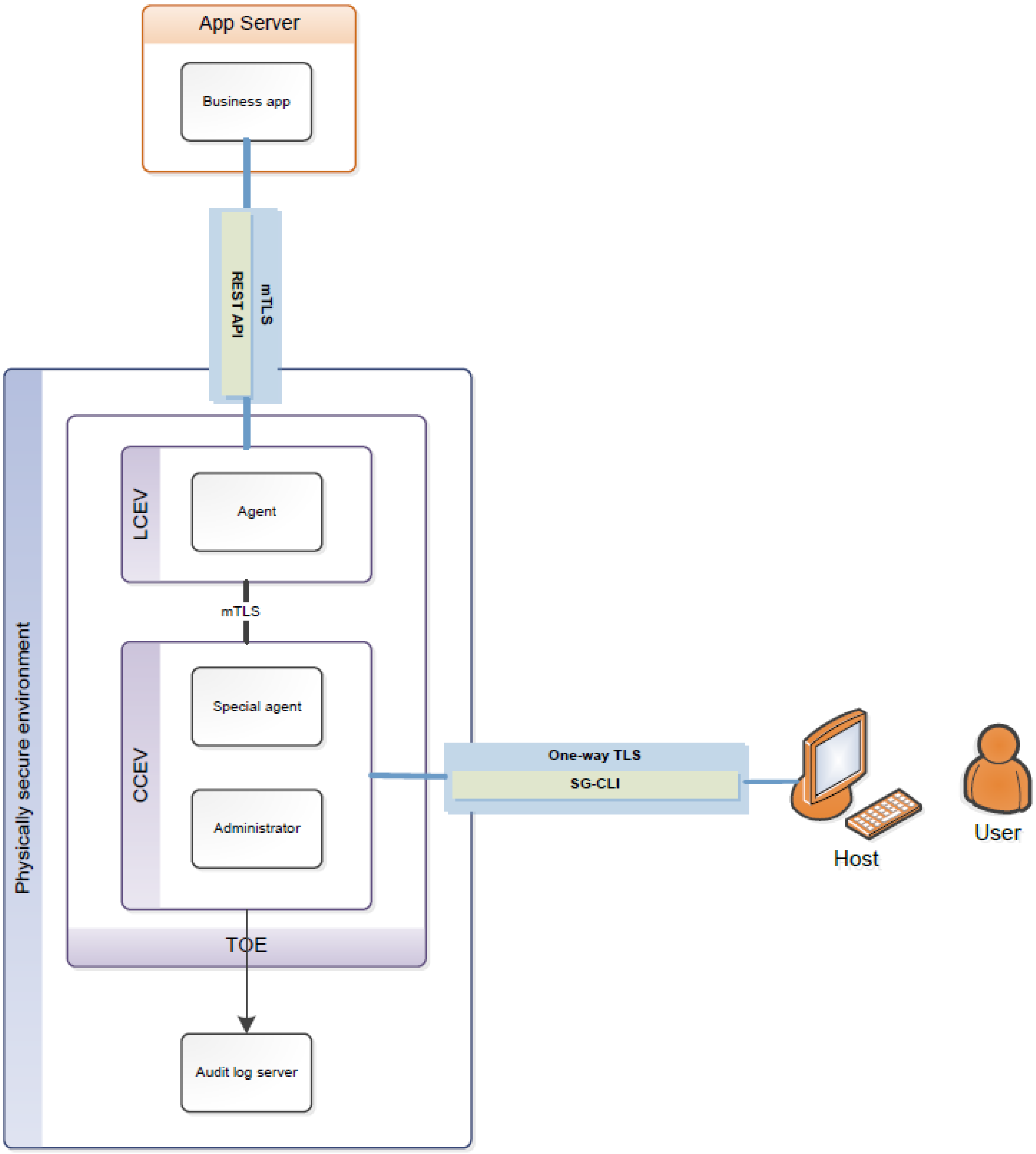

Figure 1 - Evaluated Configuration

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 additional components for its operation. These non-TOE components include:

- **SGX-enabled Intel Processors** are the main requirement as the TOE runs on such processors.
- **An Audit Log server** to record administrators' activities in CCEV. The server is logically separated from the CCEV and LCEV server. It can also be deployed in a physically separated server from the CCEV server.

- **Smart cards** come in two forms, namely administrator smart card and emergency smart card. An administrator smart card stores the administrator's public certificate. An emergency smart card stores a share of the backup key according to Shamir Secret Sharing scheme.
- **A dedicated smart card reader** connects to the CLI.
- **Red Hat Enterprise Linux 8.4 operating system** with all security patches installed.
- **SG-KMS SDK** is **optional** for users. SG-KMS SDK is available in Java.
- **Network Time Protocol (NTP)** is used by the TOE for timestamping.

6 Architecture Design Information

As described in the Security Target *[1]*, the high-level logical architecture of the TOE can be depicted as follows:

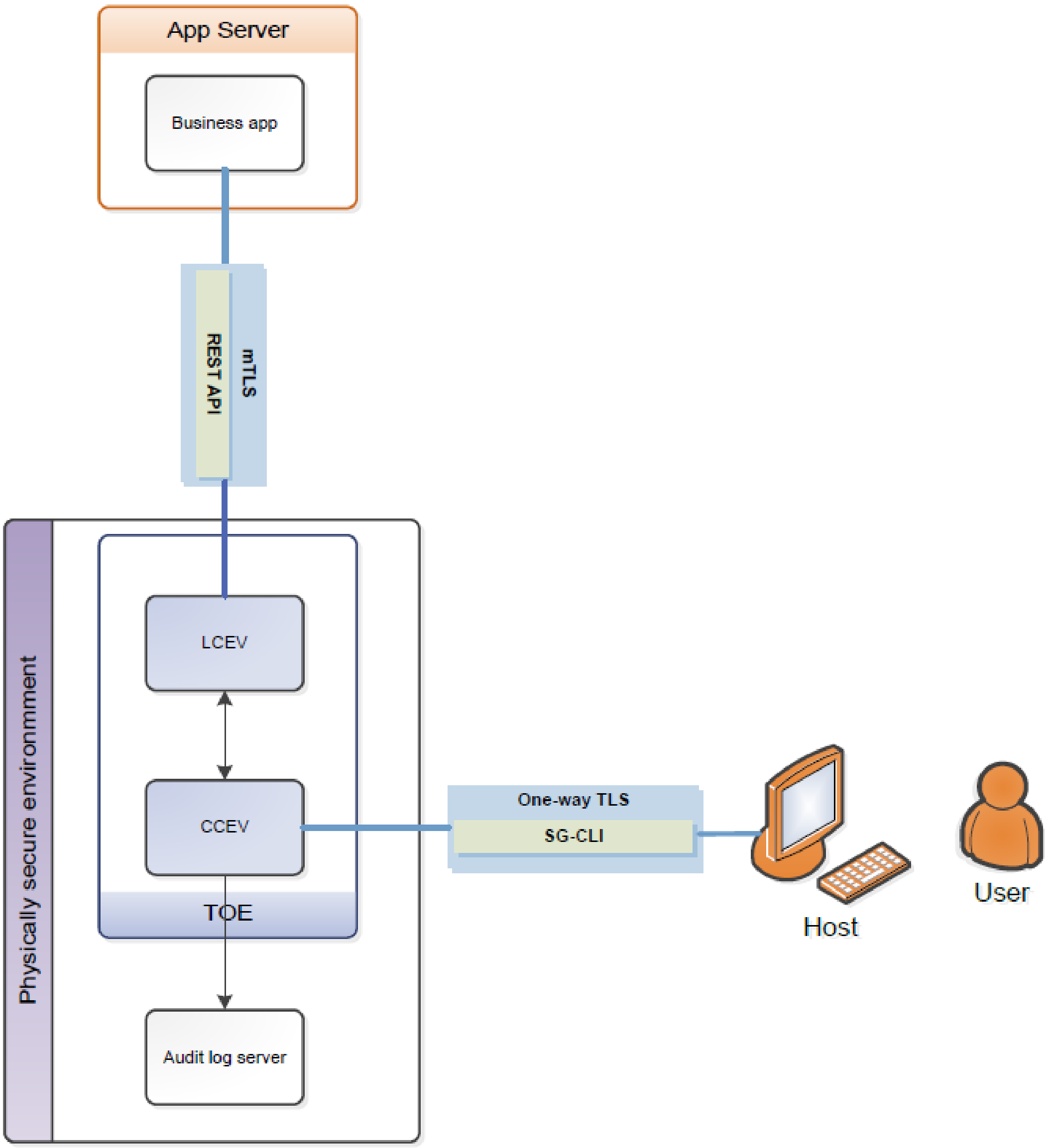

Figure 2 - Logical Architecture of the TOE

Subsytem	
CCEV	This subsystem provides key management services to TOE users, in this case, human users. The subsystem implements SG-CLI, which is a user interface for TOE users to access its key management services. To ensure secure communication between host machine and TOE, the subsystem encapsulates the SG-CLI communication with one-way TLS.
LCEV	This subsystem provides cryptographic services to TOE users, in this case, business application. The subsystem implements Rest API, which is a user interface for TOE user to access its cryptographic services. To ensure secure communication between business application and TOE, the subsystem encapsulates the Rest API communication within mTLS.

Table 8 – Subsystem description

7 Documentation

The evaluated documentation as listed in 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 documents [9] [10] [11] [12].

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

Based on Figure 2, the evaluator identified 2 TSFIs i.e, SG-CLI operating over one-way TLS and Rest API operating over mTLS. These TSFIs are exposed to threats from threat agents; other interfaces are made inaccessible by

OE.COMPET_USERS, OE.PHYSICAL_ENV and OE.IT_SUPPORT_COMP.

The evaluator sampled and repeated developer's test cases that are related to the correctness of these TSFIs.

During ATE, the evaluator devised test subsets to augment and supplement the developer's test cases to further gain assurance of the correctness of the TSFIs.

The evaluator's strategy for devising independent tests was based on the following:

- Analysis of ADV_FSP
- Analysis of ADV_TDS
- Analysis of AGD_OPE

8.2.2 Test Configuration

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

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 using public sources of information like the Common Vulnerabilities and Exposures (CVE). The following keywords were used during the search:

- Sandhiguna. This is the developer's name.
- SG-KMS. This is the TOE product name.
- SG-CLI. This is one of the TSFIs name.
- TLS 1.3. This search term is used because the evaluator understands that the TOE implements TLS 1.3 on one-way TLS and mTLS.

The OWASP Top 10 list of common web application security risks was also used to identify types of vulnerabilities.

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
VA1	Perform buffer overflow attack over mTLS and one-way TLS on the TCP layer.
VA2	Replay attack on one-way TLS to bypass the user identification/authentication TSF when issuing SG-CLI “Add Key” command.
VA3	Replay attack on REST API /var1/login command to bypass the user identification/authentication TSF.
VA4	Replay attack on one-way TLS to bypass the user identification/authentication TSF when issuing SG-CLI “Update Key” command.
VA5	Replay attack on REST API /var1/encrypt command to bypass the user identification/authentication TSF.
VA6	Fuzz mTLS and one-way TLS interface with tlsfuzzer.
VA7	Fuzzing SG-CLI with naughty string. This provides assurance that the error handling of user identification/authentication and access control TSFs are robust, in turn, resistant to bypassing.

Table 9 - Penetration Test Case

No exploitable vulnerabilities were found in the TOE when operated in the evaluated configuration. No residual risks were identified.

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.1 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.

No additional recommendation was provided by the evaluators.

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] Sandhiguna, “SG-KMS Security Target Version 1.5,” 28 August 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] Sandhiguna, “System Administrator Guide v1.0.0012-GA,” January 2023.

[10] Sandhiguna, “Deployment Guide v1.0.0012-GA,” January 2023.

[11] Sandhiguna, “SGCLI Deployment Guide v1.0.0012-GA,” January 2023.

[12] Sandhiguna, “sgkms_api_v1.0.0012_GA”.

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