

C149 Certification Report

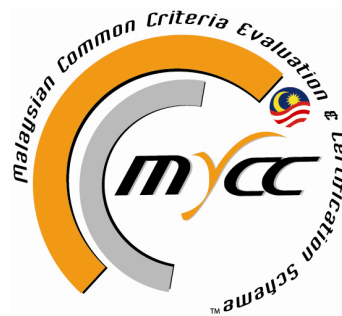
CryptoSeal Server Version 1.1

File name: ISCB-5-RPT-C149-CR-v1

Version: v1

Date of document: 10 September 2026

Document classification : PUBLIC



For general inquiry about us or our services,
please email: mycc@cybersecurity.my

C149 Certification Report

CryptoSeal Server Version 1.1

10 September 2026

ISCB Department

CyberSecurity Malaysia

Level 7, Tower 1,
Menara Cyber Axis, Jalan Impact,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 7999 □ Fax: +603 8008 7000
<http://www.cybersecurity.my>

Document Authorisation

DOCUMENT TITLE: C149 Certification Report

***DOCUMENT
REFERENCE:*** ISCB-5-RPT-C149-CR-v1

ISSUE: v1

DATE: 10 September 2026

DISTRIBUTION: UNCONTROLLED COPY - FOR UNLIMITED USE AND
DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2026

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 200601006881 (726630-U)

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the MyCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

The Certification Report, Certificate of the evaluated product, and the Security Target (Ref [5]) have been published on the MyCC Scheme Certified Product Register (MyCPR) at <https://iscb.cybersecurity.my> and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme using the Common Methodology for IT Security Evaluation, version 2022 revision 1 (Ref[3]), for conformance to the Common Criteria for IT Security Evaluation, version 2022 revision 1 (Ref[2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
d1	24 August 2026	All	Initial draft
d2	02 September 2026	All	1) Change on the foreword 2) Include the Security Function in the Executive Summary 3) Added the Threats in Section 1.7 4) Added the Manual Document in Section 2.1.3 5) Correcting all the reference number and grammatical error in all sections.
v1	10 September 2026	All	Final Version

Executive Summary

The project is C149 CryptoSeal Server Version 1.1, referred to as the Target of Evaluation (TOE) which developed by Zetvest Sdn. Bhd. The TOE is a server-based centralized management system deployed within an organization's information technology infrastructure. It provides administrative functions for managing organizational structures, user identities, device registration records, and license information within the operational environment.

The TOE provides security functions such as Identification and Authentication, Security Management, Security Audit and Secure Communication.

The scope of the evaluation is defined by the Security Target (Ref[6]) which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 2. This report confirms that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysia Common Criteria Evaluation and Certification (MyCC) Scheme (Ref[4]).

The evaluation was performed by Securelytics Security Evaluation Facility (SEF) and the evaluation was completed on 15 August 2026.

This Certification Report is associated with the Certificate of Product Evaluation (2026-003-C149) dated 18 September 2026 and the Security Target (Ref[6]). The certification is valid for a period of five (5) years from the date of the Certificate of Product Evaluation, after which it will expire.

It is the responsibility of the user to ensure that CryptoSeal Server Version 1.1 meets their requirements. It is recommended that a potential user of the TOE refer to the Security Target (Ref[6]) and this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Document Authorisation.....	ii
Copyright Statement.....	iii
Foreword	iv
Disclaimer	v
Document Change Log	vi
Executive Summary	vii
Index of Tables	ix
1 Target of Evaluation.....	1
1.1 TOE Description	1
1.2 TOE Identification.....	2
1.3 Security Policy	2
1.4 TOE Architecture	3
1.4.1 Logical Boundaries	3
1.4.2 Physical Boundaries.....	4
1.5 Clarification of Scope.....	5
1.6 Assumptions	5
1.6.1 Operational Environmental assumptions	5
1.7 Threats.....	6
1.8 Evaluated Configuration	6
1.8.1 Evaluated Server-Side Configuration	6
1.8.2 Evaluated Client-Side Configuration.....	6
1.8.3 Evaluated Cryptographic Configuration	7
1.9 Delivery Procedures	7
1.9.1 TOE Delivery Procedures	7
1.9.2 Delivery to Customers.....	7
2 Evaluation.....	9
2.1 Evaluation Analysis Activities	9

2.1.1	Life-cycle support	9
2.1.2	Development	9
2.1.3	Guidance documents	10
2.1.4	IT Product Testing	10
3	Result of the Evaluation	17
3.1	Assurance Level Information.....	17
3.2	Recommendation	17
Annex A	References.....	19
A.1	References	19
A.2	Terminology.....	19
A.2.1	Acronyms.....	19
A.2.2	Glossary of Terms	20

Index of Tables

Table 1: TOE Identification	2
Table 2: Assumptions for the TOE Environment.....	5
Table 3 : Threats for the TOE	6
Table 4 : Independent Functional Test.....	14
Table 5 : List of Acronyms.....	19
Table 6 : Glossary of Terms.....	20

1 Target of Evaluation

1.1 TOE Description

- 1 The CryptoSeal Server Version 1.1 is a server-based centralized management system deployed within an organization's information technology infrastructure. It provides administrative functions for managing organizational structures, user identities, device registration records, and license information within the operational environment.
- 2 The TOE is deployed on a physical or virtual server and includes a web-based portal through which TOE users perform the TOE operations. The TOE enables centralized control and administration of system entities and management data, supporting consistent configuration and oversight across TOE users and devices.
- 3 The primary features of the TOE are:
 - Web-Based Portal – Provides a browser-accessible web portal for TOE users to perform management and configuration activities.
 - Organization Management – Provides functionality to create, modify, and manage organizational entities within the system.
 - License Management – Enables management of license information and subscription details.
 - User Management – Supports creation, modification, and maintenance of user accounts.
 - Group Management – Provides functionality to define and manage user groups and associated role assignments.
 - Device Management – Enables registration and management of device records within the system.
- 4 The TOE can be categorised as Other Devices and Systems in accordance with the categories identified in the Common Criteria Portal.
- 5 The TOE implement the following security functions:
 - Identification & Authentication – The TOE requires that each TOE user is successfully identified and authenticated before any interaction with protected resources is permitted.
 - Security Management – The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.
 - Security Audit – The TOE generates audit records for security events.
 - Secure Communication– The TOE able to protect the user data and transaction from disclosure and modification by using HTTPS (TLS v1.2 and TLS v1.3).

1.2 TOE Identification

6 The details of the TOE are identified in table below.

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C149
TOE Name	CryptoSeal Server
TOE Version	Version 1.1
Security Target Title	CryptoSeal Server Version 1.1 Security Target
Security Target Version	v1.0
Security Target Date	27 July 2026
Assurance Level	Evaluation Assurance Level 2
Criteria	Common Criteria for Information Technology Security Evaluation, November 2022, Version 2022, Revision 1 (Ref[2])
Methodology	Common Methodology for Information Technology Security Evaluation, November 2022, Version 2022, Revision 1 (Ref[3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant
Sponsor	Zetvest Sdn Bhd Unit 208, Block B, Phileo Damansara 2, Jalan 16/11, 46350 Petaling Jaya, Selangor, Malaysia
Developer	Zetvest Sdn Bhd Unit 208, Block B, Phileo Damansara 2, Jalan 16/11, 46350 Petaling Jaya, Selangor, Malaysia
Evaluation Facility	Securelytics SEF A-19-06, Tower A, Atria SOFO Suites, Jalan SS 22/23, Damansara Utama, 47400 Petaling Jaya, Selangor, Malaysia

Table 1: TOE Identification

1.3 Security Policy

7 No Organisational Security Policy (OSP) declared for the TOE.

1.4 TOE Architecture

- 8 The TOE consist of logical and physical boundaries which are described in Section 1.6 of the Security Target (Ref[6]).

1.4.1 Logical Boundaries

- 9 The logical boundary of the TOE is summarized below:

- **Identification & Authentication**

TOE users are required to be identified and authenticated before any information flows are permitted. At the login page, TOE users need to enter a valid email and password in order to access the TOE. Passwords must be at least 8 characters long and include at least one uppercase letter, one lowercase letter, one number, and one special character (@\$!%*?&_). The TOE checks the credentials presented by the user against the authentication information stored in the database.

- **Security Management**

The TOE contains various management functions to ensure efficient and secure management of the TOE. The TOE restricts access to the management functions based on the role of the user. The TOE defines six (6) user roles which are Super Admin, System Admin, License Admin, User Admin, Reporting Admin and End User each with specific responsibilities.

- **Security Audit**

The TOE generates audit records for security events.

Super Admin and System Admin can view and export audit logs such as:

- Access Log
- Failed Log
- User Activity
- Desktop Activity
- System Log

Reporting can view and export audit logs such as:

- Access Log
- Failed Log
- User Activity

- System Log
- **Secure Communication**

The TOE can protect the user data and transactions from disclosure and modification by using HTTPS (TLS v1.2 and TLS v1.3)

1.4.2 Physical Boundaries

- 10 A typical implementation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

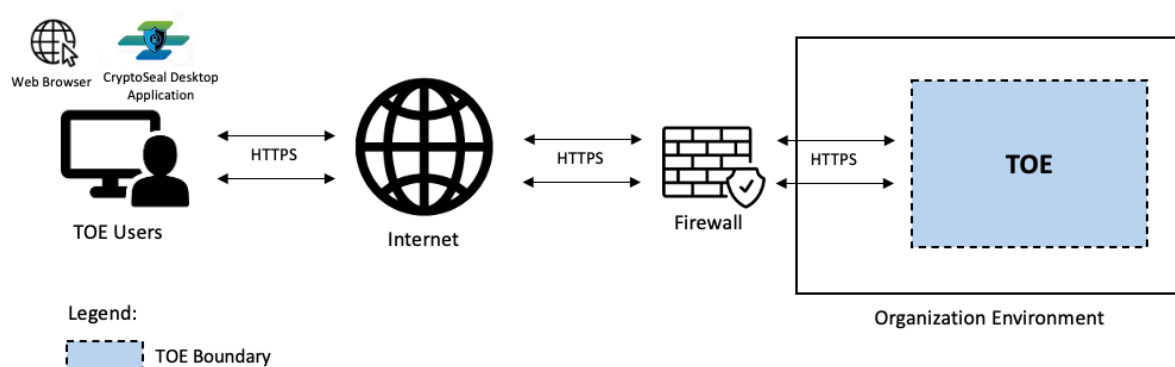


Figure 1: TOE

- 11 The TOE is part of the CryptoSeal technology suite, which consists of CryptoSeal Server Version 1.1 (the TOE) and the CryptoSeal Desktop Application. In an enterprise deployment, the TOE resides within the organization's controlled environment, such as on-premises data centre or private cloud infrastructure. The CryptoSeal Desktop Application is outside the scope of evaluation.
- a) **Web Browser:** The TOE provides a web-based portal that allows TOE users to perform operations using a standard web browser stated in Section 1.5.3 Security Target. The TOE users are created and managed within the TOE. Credentials generated and maintained by the TOE are used by those users to authenticate when accessing the CryptoSeal Desktop Application. The TOE also manages license information, including licenses that authorize the use of the CryptoSeal Desktop Application, and maintains device registration records for devices permitted to access the CryptoSeal Desktop Application.
 - b) **CryptoSeal Desktop Application:** CryptoSeal desktop application is a desktop-based cryptographic application that enables application users to perform encryption and decryption on files and directories using AES-256, Threefish

and Chacha20 algorithm. The application allows application users to encrypt and decrypt single files, multiple files, or entire directories.

1.5 Clarification of Scope

- 12 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.
- 13 Section 1.4 of this document describes the scope of the evaluation, which is limited to those claims made in the Security Target (Ref[6]).
- 14 Potential consumers of the TOE are advised that some functions and services of the overall product have not been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

- 15 This section summarises the security aspects of the environment/configuration in which the product is intended to operate. Consumers should understand the requirements for secure operation of the TOE as defined in the Security Target (Ref[6]).

1.6.1. Operational Environmental assumptions

- 16 Assumptions for the TOE environment as described in the Security Target (Ref [5]):

Environment	Statement
A.NOEVIL	It is assumed that the person who manages the TOE is not hostile and is competent.
A.AUTHORISE	It is assumed that the TOE can only be accessed by authorized TOE users.
A.TIMESTAMP	It is assumed that the operational environment is capable of providing reliable timestamps for the TOE
A.UPDATE	It is assumed that the developer will regularly apply security patches and updates to the TOE and the underlying platform.
A.FIREWALL	It is assumed that the firewall should be able to provide gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE.

Table 2: Assumptions for the TOE Environment

1.7 Threats

17 Threats for the TOE as address in the Security Target (Ref[6]):

Identifier	Threat Statement
T.COMINT	An unauthorised user may attempt to disclose or modify data transmitted between distributed TOE components, thereby compromising the confidentiality of the communication.
T.DISCLOSURE	An unauthorised user may attempt to compromise the integrity of the protected resource on the TOE.
T.IMPERSON	An attacker may gain unauthorised access to information or resources by impersonating an authorised user of the TOE.
T.PASSWORD	An unauthorized user may take advantage of weak administrative passwords to gain privileged access to the TOE functions.
T.NOMGMT	An unauthorized person modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.

Table 3 : Threats for the TOE

1.8 Evaluated Configuration

18 The TOE was evaluated in a defined and controlled configuration. The evaluation results presented in this report apply only to the TOE when installed, configured, and operated in accordance with this evaluated configuration. Any other configurations are outside the scope of this evaluation.

1.8.1 Evaluated Server-Side Configuration

19 During evaluation, the TOE was installed and operated on the following server configuration (minimum requirement):

- Operating System: Ubuntu Server 24.04, Red Hat Enterprise Linux 9 APIs.
- Processor: Intel Core i7-10700K 8 cores / 16 threads x86 & 64 architecture
- Memory: 32 GB RAM
- Storage: 1 TB

1.8.2 Evaluated Client-Side Configuration

20 The TOE was accessed by users using the following client configuration (minimum requirement):

- Operating System: Windows 11
- Web Browsers:
 - Chrome 148
 - Safari 26
 - Firefox 150
 - Microsoft Edge 148

1.8.3 Evaluated Cryptographic Configuration

- 21 The TOE was evaluated with the following cryptographic mechanism enabled:
- TLS v1.2 and TLS v1.3 to provide trusted communication paths between the TOE and TOE users
- 22 These cryptographic mechanisms support the security functional requirements defined in the ST which is secure communication.

1.9 Delivery Procedures

- 23 The evaluators examined the delivery documentation and determined that it describes all procedures that are necessary to maintain security when distributing versions of the TOE or parts of it to the consumer.
- 24 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.9.1 TOE Delivery Procedures

- 25 The TOE is delivered and deployed only by authorized representatives from Zetvest. The TOE is implemented as a server-based centralized management system deployed on either a physical server or a virtual server environment within the TOE users infrastructure. The TOE is packaged in sealed protective packaging to provide resistance against moisture. Each TOE is then enclosed in a cardboard shipping box and sealed using Zetvest-labelled packaging tape to provide visible evidence of tampering. A shipping label identifying the exact product (including the serial number of the included device) and the customer's name is affixed to the outside of the box.

1.9.2 Delivery to Customers

- 26 To maintain the integrity and authenticity of the TOE during delivery and deployment, the following controls are applied:

- Delivery of the TOE is coordinated directly between Zetvest and the TOE Users.
- Ensuring that the underlying software/hardware platforms meet the required specifications; A schedule is given to customers via email regarding the delivery of the TOE to allow customer to know when the TOE is expected to be delivered by the Authorized Representative from Zetvest.
- The TOE configuration will be performed by the authorized representative from Zetvest. The configuration process includes the TOE configuration, credentials configuration, IP address, zone upload and license generation.
- Default accounts and passwords are created by authorized representative from Zetvest.
- The TOE deployment package and installation media are handled only by authorized personnel from Zetvest.
- The TOE is deployed directly into the TOE users designated server environment by the authorized representative from Zetvest.
- TOE installation and initial configuration activities are performed only by authorized representatives from Zetvest to reduce the risk of unauthorized modification or substitution of the TOE.
- Super Admin is required to verify the delivery details and deployment environment prior to installation.
- Any unexpected modification, damaged packaging, or discrepancy identified during delivery or deployment must be reported to Zetvest immediately and deployment activities must be suspended until verification is completed.

2 Evaluation

- 27 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 2022 Revision 1 (Ref[2]) and the Common Methodology for IT Security Evaluation (CEM), version 2022 Revision 1 (Ref[3]). The evaluation was conducted at Evaluation Assurance Level 2. The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref[4]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref[5]).

2.1 Evaluation Analysis Activities

- 28 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

- 29 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.
- 30 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

- 31 The evaluators analyzed the TOE functional specification; they determined that the design completely and accurately describes the TOE security functionality interfaces (TSFIs), and how the TOE security function (TSF) implements the security functional requirements (SFRs).
- 32 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behavior of the SFR-enforcing subsystems.

- 33 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.
- 34 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

- 35 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.
- 36 The documents for TOE users to refer as guidance are as per listed:
- CryptoSeal Server Version 1.1 Manual Version 0.2 date 22 June 2026
- 37 The evaluators confirmed that the TOE guidance has fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

- 38 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Securelytics SEF. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Report.

2.1.4.1 Assessment of Developer Tests

- 39 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator). The results of the evaluators tests are consistent with the developers test results defined in their evaluation evidences submitted.

2.1.4.2 Independent Functional Testing

- 40 At EAL 2, independent functional testing is the evaluation conducted by evaluators based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a subset of the developer's test plan, and creating test cases that are independent of the developer's tests.
- 41 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The results of the independent functional tests were recorded by the evaluators and are consistent with the expected test results in the test documentation.

Test ID	Description	Security Function	Results
F001 – Security Audit & User Data Protection	1. To test that the TOE be able to generate an audit data of the following auditable events: a) Start-up and shutdown of the audit functions b) All auditable events for the [not specified] level of audit c) Specifically defined auditable events listed in the Notes section 5.2.2 in ST Ref [6]) 2. To test that the TOE record within the audit data at least the following information: a) Date and time of the auditable event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event. b) For each auditable event type, based on the auditable event definitions of the functional components included in the PP, PP-Module, functional package or ST. 3. To test that the TOE provide Super Admin, System Admin and Reporting Admin with the capability to read and export [audit information stated in	FAU_GEN.1.1, FAU_GEN.1.2, FAU_SAR.1.1, FAU_SAR.1.2, FDP_ACF.1.1, FDP_ACF.1.2, FDP_ACF.1.3, FDP_ACF.1.4	Passed

Test ID	Description	Security Function	Results
	Table 1 section 5.2.3 in ST (Ref.[6]) from the audit data. 4. To test that the TOE provide the audit data in a manner suitable for the user to interpret the information. 5. To test that the TOE enforce the [access control SFP] to objects based on the following: [as listed in the Table 1 section 5.2.3 in ST (Ref.[6]). 6. To test that the TOE enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [a) If the TOE user is successfully authenticated accordingly, then access is granted based on privilege allocated; b) If the TOE user is not authenticated successfully, therefore, access permission is denied.] 7. To test that the TOE explicitly authorize access of subjects to objects based on the following additional rules: [none]. 8. To test that the TOE explicitly deny access of subjects to objects based on the following additional rules: [none].		
F002 – Security Management & User Data Protection	1. To test that the TOE be capable of performing the following management functions: [all management functions stated in Table 13 section 5.2.4 in ST (Ref.[6]). 2. To test that the TOE enforce the [access control SFP] to provide	FMT_SMF.1.1, FMT_MSA.3.1, FMT_MSA.3.2, FMT_SMR.1.1, FMT_SMR.1.2, FDP_ACC.1.1	Passed.

Test ID	Description	Security Function	Results
	[restrictive] default values for security attributes that are used to enforce the SFP. 3. To test that the TOE allow the [none] to specify alternative initial values to override the default values when an object or information is created. 4. To test that the TOE maintain the roles [Super Admin, System Admin, License Admin, User Admin, Reporting Admin, End User]. 5. To test that the TOE be able to associate users with roles. 6. To test that the TOE enforce the [access control SFP] on [objects listed in the Table 13 section 5.2.4 in ST (Ref.[6])]		
F003 – Security Management	To test that the TOE enforce the [access control SFP] to restrict the ability to [change_default, modify, delete] the security attributes [all organization information] to [Super Admin].	FMT_MSA.1.1	Passed.
F004 – Security Management	To test that the TOE restrict the ability to [modify] the [Super Admin Password] to [Super Admin].	FMT_MTD.1.1	Passed.
F005 – Identification and Authentication	1. To test that the TOE maintain the following list of security attributes belonging to individual users: a) Email, b) Password 2. To test that the TOE provide a mechanism to verify that secrets meet	FIA_UAU.2.1, FIA_UID.2.1	Passed.

Test ID	Description	Security Function	Results
	[a minimum length of 8-characters, contain at least one uppercase letter, one lowercase letter, one number, and one special character (@\$!%*?&_).		
F006 – Identification and Authentication	1. To test that the TOE require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. 2. To test that the TOE require each user to be successfully identified before allowing any TSFmediated actions on behalf of that user.	FIA_UAU.2.1, FIA_UID.2.1	Passed.
F007 – Identification and Authentication	To test that the TOE re-authenticate the user under the conditions [no user interaction has been detected over 15 minutes].	FIA_UAU.6.1	Passed.
F008 – Trusted Path	1. To test that the TOE provide a communication path between itself and [remote] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [modification or disclosure]. 2. To test that the TOE permit [remote users] to initiate communication via the trusted path. 3. To test that the TOE require the use of the trusted path for [initial user authentication, [and all further communication after authentication].	FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3	Passed.

Table 4 : Independent Functional Test

- 42 All testing performed by evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Vulnerability Analysis

- 43 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, implementation representation and security architecture description.
- 44 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attack performed by an attacker possessing a Basic attack potential. The following factors have been taken into consideration during penetration tests:
- a) Time taken to identify and exploit (elapsed time);
 - b) Specialist technical expertise required (specialised expertise);
 - c) Knowledge of the TOE design and operation (knowledge of the TOE);
 - d) Window of opportunity; and
 - e) IT hardware/software or other equipment required for exploitation

2.1.4.4 Vulnerability testing

- 45 The penetration tests focused on:
- a) Broken Access Control
 - b) Security Misconfiguration
 - c) Software Supply Chain Failures
 - d) Cryptographic Failures
 - e) Injection
 - f) Authentication Failures
 - g) Software or Data Integrity Failures
 - h) Security Logging and Alerting Failures
 - i) Mishandling of Exceptional Conditions
- 46 The result of the penetration testing noted that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in the Security Target (Ref[6]).

2.1.4.5 Testing Results

- 47 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification. Therefore, the certifiers confirmed that all the test conducted were **PASSED** as expected.

3 Result of the Evaluation

- 48 After due consideration during the oversight of the execution of the evaluation by the certifiers and review of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies that the evaluation of CryptoSeal Server Version 1.1, performed by Securelytics SEF, has been completed with a PASS verdict.
- 49 Securelytics SEF found that CryptoSeal Server Version 1.1 upholds the claims made in the Security Target (Ref[6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2.
- 50 Certification does not guarantee that a TOE is completely free from exploitable vulnerabilities. A residual level of risk remains that previously undiscovered exploitable vulnerabilities may exist within its claimed security functionality. However, this risk is reduced as the assurance level achieved by the TOE increases.

3.1 Assurance Level Information

- 51 EAL 2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using functional and interface specifications, guidance documentation and a description of the design of the TOE and the implementation to understand the security behaviours.
- 52 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 penetration attackers with a **Basic** attack potential.
- 53 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

- 54 The Malaysian Certification Body (MyCB) is strongly recommended that:
- a) The users should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

- b) The users must maintain the confidentiality, integrity, and availability of security relevant data for TOE initialization, start-up and operation if stored or handled outside the TOE.
- c) The users must ensure appropriate network protection is maintained, the network on which the TOE is installed must be both physically and logically protected.

(Disclaimer: Opinion and interpretations expressed herein are outside the scope of certification)

Annex A References

A.1 References

- [1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.
- [2] The Common Criteria for Information Technology Security Evaluation, Version 2022, Revision 1, November 2022.
- [3] The Common Methodology for Information Technology Security Evaluation, Version 2022, Revision 1, November 2022.
- [4] MyCC Scheme Requirement (MYCC_REQ), V2, April 2025.
- [5] ISCB Evaluation Facility Manual (ISCB_EFM), v4, April 2025.
- [6] CryptoSeal Server Version 1.1 Security Target, v1.0, 27 July 2026.
- [7] Evaluation Technical Report, Version 1.0, 15 August 2026.

A.2 Terminology

A.2.1 Acronyms

Table 5 : List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 6 : Glossary of Terms

Term	Definition and Source
CC International Interpretation	An interpretation of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out certification and for overseeing the day-to-day operation of an Evaluation and Certification Scheme . Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS-ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of evaluation and certification under the authority of a certification body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a national interpretation or a CC international interpretation .
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An interpretation of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---