MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity MALAYSIA

C127 Certification Report

Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24

File name: ISCB-5-RPT-C127-CR-v1.1
Version: v1.1
Date of document: 29 August 2022
Document classification : PUBLIC

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

CyberSecurity Malaysia
(726630-U)
T +603 8800 7999
F +603 8008 7000
H 1 300 88 2999

Corporate Office:
Level 7, Tower 1
Menara Cyber Axis
Jalan Impact
63000 Cyberjaya
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C127 Certification Report

Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24

29 August 2022

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:	C127 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C127-CR-v1.1
ISSUE:	v1.1
DATE:	29 August 2022
DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 7, Tower 1

Menara Cyber Axis

Jalan Impact

63000 Cyberjaya

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 201601006881 (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.

This certification report is associated with the certificate of product evaluation dated 12 August 2022, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement).

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 3.1 revision 5 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 5 (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	25 July 2022	All	Initial draft
v1	5 August 2022	All	Final version
v1.1	29 August 2022	All	Edit TOE name (CSS to CCS)

Executive Summary

The Target of Evaluation (TOE) is a privileged Access Management (PAM) called Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24 that offer user to perform authentication without password. The TOE offer end users to use their own mobile device to perform a one-click passwordless authentication to verify their credentials, only username or user ID is required during authentication and identification process. BSA Server consists of three (3) components which is the web server, Guardian-CCS BSA (API) and database. TOE for this evaluation will only focus on the API engine that used by Guardian-CCS BSA to identify and authenticate user.

The TOE provides security features such as User Data Protection, Identification and Authentication, Security Management and TOE Access.

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 (EAL2). 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 Cybertronics Lab and the evaluation was completed on 25 July 2022.

The Malaysia Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at http://www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at http://www.commoncriteriaportal.org

It is the responsibility of the user to ensure that Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24 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

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) a privileged Access Management (PAM) system called Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24 that offer user to perform authentication without password.

2 Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24 is an identity authentication platform that relies on patented hybrid blockchain technology to provide an unbreakable, fast and easy-to-use solution to meet all security needs.

3 Users is allowed to perform one-click authentication on their mobile device to login into respective application with presence of valid User ID and TOE. Besides that, multi-factor authentication is required to initiate for identification process.

4 The BSA Server consist of web server, Guardian-CCS BSA (API) and database. For this evaluation and certification, only focus on the API engine that used by Guardian-CCS BSA to identify and authenticate user.

5 Guardian-CCS BSA (API) is utilized to perform the following process:

a) Create or Delete Authentication Key

b) Node Verification

c) Device Verification

d) Encrypt and Hash Data

6 In traditional implementations, clients or customers will need to have a set of credentials (e.g., usernames and password) to login into the systems and this may lead to a burden for customers or clients to remember their password.

7 Losing the password would require customers to go through the hassle of resetting or retrieval of password.

8 This also can lead to unnecessary exposure to security leakages if credentials are used repeatedly.

9 Unauthorized users may obtain access to the system with the stolen credentials from legitimate users.

10 This TOE can prevent account takeovers and credential stuffing attacks by implementing passwordless authentication.

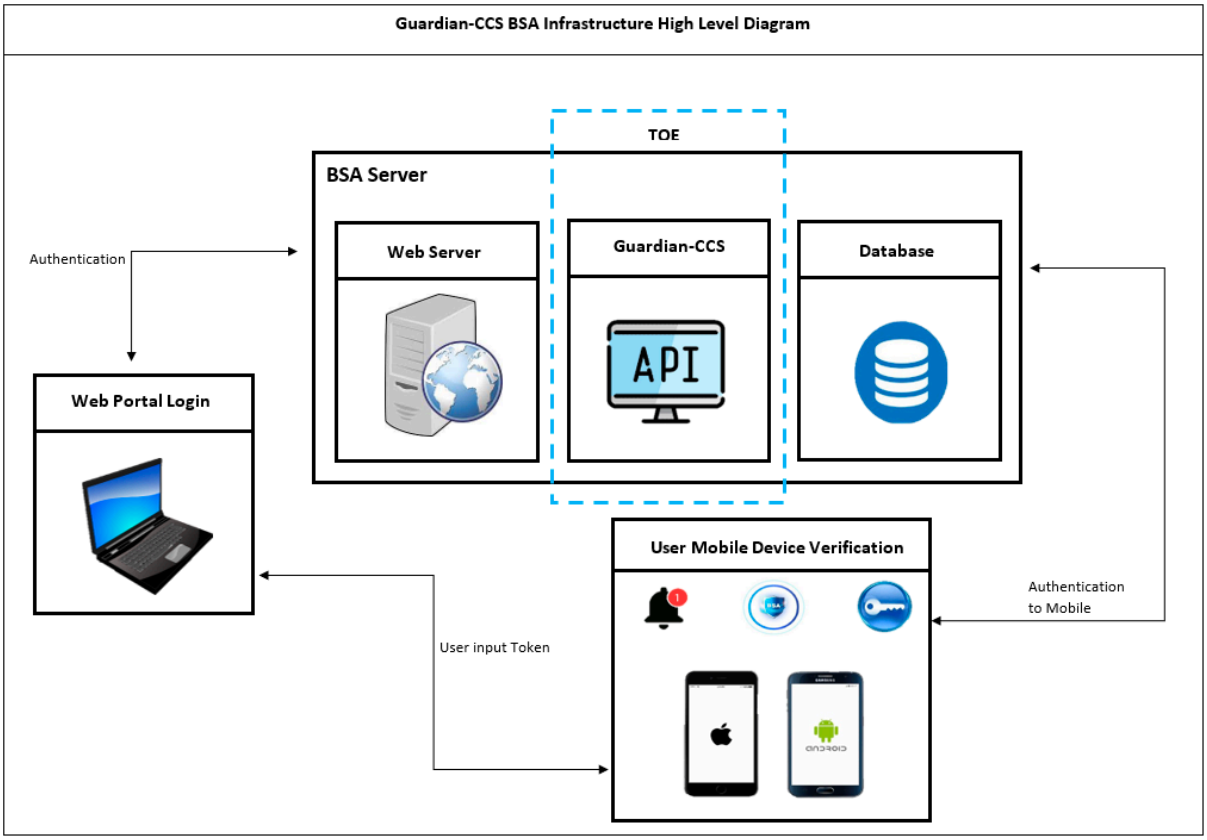

Figure 1: Guardian-CCS BSA High Level Diagram

1.2 TOE Identification

11 The details of the TOE are identified in Table 1: TOE Identification below.

Table 1: TOE Identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C127
TOE Name	Guardian-CCS Blockchain Secure Authentication (BSA)
TOE Version	V1.0.24
Security Target Title	FNS - Guardian - CCS Blockchain Secure Authentication (BSA)Security Target
Security Target Version	V1.2
Security Target Date	29 August 2022
Assurance Level	Evaluation Assurance Level 2

Criteria	Common Criteria for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, April 2017, Version 3.1, Revision 5 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 2
Sponsor	FNS (M) Sdn Bhd Office Suite 5.01, Level 5 Menara LGB, No.1, Jalan Wan Kadir Taman Tun Dr Ismail 60000 Kuala Lumpur, Malaysia. Tel: +603-7732 6027 Website: https://fnsmalaysia.com/
Developer	FNS (M) Sdn Bhd Office Suite 5.01, Level 5 Menara LGB, No.1, Jalan Wan Kadir Taman Tun Dr Ismail 60000 Kuala Lumpur, Malaysia. Tel: +603-7732 6027 Website: https://fnsmalaysia.com/
Evaluation Facility	Cybertronics Lab C-5-15, Centum @ Oasis Corporate Park No 2, Jalan PJU 1A/2, Ara Damansara 47301 Selangor, Malaysia Tel: +603-7627 4060 Fax: +603-7627-4070 Website: https://www.acrossverticals.com

1.3 Security Policy

12 P. Role: Only authorized user assigned by the organization have access to the TOE and TOE environment

1.4 TOE Architecture

13 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

14 The logical boundary of the TOE is summarized below:

- User Data Protection
    - User data and credentials are protected by ensuring that specific users within the system are assigned with specific roles and privilege access to the TOE. The accessibility to the web portal is protected based on the access control policy.
    - The TOE can identify and authenticate the credentials of users before allowing the users to access the web portal. TOE will identify the user based on the User ID and will request the user to proceed with the authentication process via QR Scanning, OTP or TOTP from the user's mobile device. Users who are unable to be authenticated are not allowed to access the web portal.
- Identification and Authentication
    - TOE requires users to input a valid User ID for the TOE to initiate the identification process. Users required multi-factor authentication to access the BSA mobile application and proceed to authentication process via QR scanning, OTP or TOTP. The TOE shall then authenticate the users by their respective User ID along with the random selection of user attributes in the database which will generate a token for authentication. Each user will have a unique User ID which cannot be modified after onboarding process.
- Security Management
    - FNS Manager (Super Admin) has access to all TOE features, that application to be managed through web portal hosted by FNS. FNS Manager (Super Admin) has the full access rights, role and privileges to the TOE. FNS Manager (Super Admin) could Create, View, Edit, or Delete user data via the web portal. Nonetheless, there are another 3 roles that are allows to access the TOE features, which is: Vendor Manager could View, Edit, or Delete user data via the web portal, Client Manager could View user data via the web portal and User could view their own

information. These roles are defined with limited access to the TOE features compared to the TOE FNS Manager (super admin).

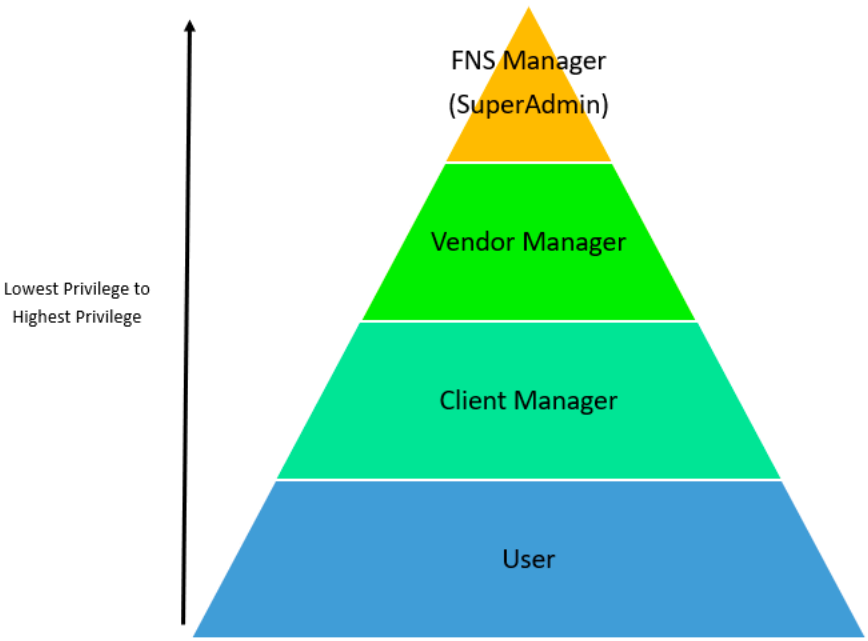

Figure 2: Hierarchy of TOE Management

- TOE Access
    - Users are allowed to check on previous successful or unsuccessful authentication attempt through the TOE. Access history is being stored in the server thus user's is not allowed to tamper or remove the access logs. Such action allows the users to review past authentication history to identify if users identify is being misused.

1.4.2 Physical Boundaries

15 As illustrated in Figure 3 the TOE consists of the following components:

a) Controller – Connector to communicate with Web and Mobile Application.

b) QR – User Identification with QR Code.

c) OTP – User Identification with One Time Password.

d) TOTP – User Identification with Time-based One-Time Password.

e) Message Service – Used to deliver OTP to the user during onboarding and identification process.

f) KnChain – Core API engine for BSA product.

g) Spring Framework – An application framework and inversion of control container for the Java platform application.

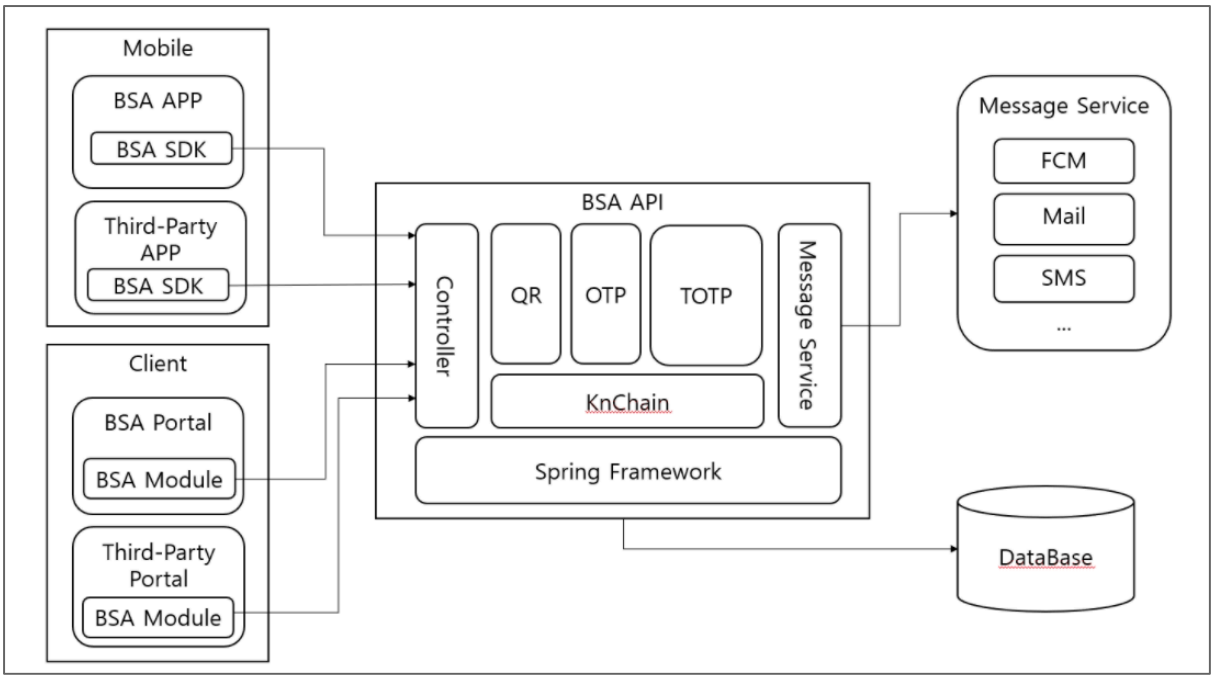

Figure 3: TOE Physical Scope

1.5 Clarification of Scope

16 The TOE is designed to be suitable for use in accordance with user guidance that is supplied with the product.

17 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]).

18 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

19 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 Environmental assumptions

20 Assumptions for the TOE environment as described in the Security Target (Ref [6]):

Table 2: Assumptions for the TOE Environment

Environment	Statement
A.USER	The users are trusted; the users shall not maliciously compromise the security functionality of the TOE. The users are well-trained; the user shall comply to the operating procedures stipulated in the user guidance.
A.ADMIN	Authorized super administrators are non-hostile and follow guidance however, they are not free from error.
A.IDLE	The TOE environment must be protected. Session timeout is imposed in client web application and mobile application for 90 seconds. It requires 2 Factor Authentication before able to generate OTP.
A.HISTORY	The TOE shall allow the users to review authentication history to identify for misuse of their user account for identification and authentication.

1.7 Evaluated Configuration

21 This section describes the configurations of the TOE is to be configured according to the Preparative Guidance.

22 a) Domain Separation

The TOE does not provide security domains to potentially harmful entities. The TOE management functionality described does not provide security domains but is a direct implementation of the security requirements. In short, security domains are not applicable for this TOE.

23 b) Initialisation

FNS Engineer will install BSA software into and guidance documents will be provided to the customer as a reference. UAT test will be perform once installation is completed and agreed by the end user.

24 c) Protection from Tampering

i) Physical Protection

TOE is a software thus Physical Protection is not applicable.

ii) Logical

Logical Protection is applicable for the TOE. Authentication and Identification before any action is required.

25 d) Protection from Bypassing:

TSF ensures that the security functionality is always invoked and hence, with the self protection (as described earlier in this document) and correct functional behaviour (as described in the FSP/TDS evaluation evidence), the SFRs are always enforced.

1.8 Delivery Procedures

26 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.

27 The evaluators also examined the aspects of the delivery process and determined that the delivery procedures are used.

1.8.1 TOE Delivery Procedures

28 The TOE is delivered by FNS personnel in maintaining security when distributing Guardian-CCS BSA to the customer:

29 The customer will purchase the product and complete the payment. Once payment is confirmed and legal documentations have been completed, FNS personnel can proceed with preparing and delivering the product.

30 FNS Personnel will make the necessary preparation for On-Prem Solution:

a) Prepare “User Roles and Menu Summary” and “User Onboarding Manual” and deliver to the customer by email.

b) FNS engineer will schedule a deployment time with customer to perform initial setup

c) FNS engineer have the installer file in USB drive and using the same USB drive to perform installation.

d) Licence Key will be entered by FNS engineer through the web portal.

e) End-user will be manually informed through E-mail once license had been entered.

f) License will be automatically activated on the start date and expired on the end-date.

31 FNS Personnel will make necessary preparation for SaaS Solution:

a) Prepare “User Roles and Menu Summary” and “User Onboarding Manual” and deliver to the customer by E-mail.

b) FNS engineer will perform initial setup at the cloud environment based on customer requirements.

c) Knowledge transfer to Customer on Configuration in SaaS.

32 Once the package is delivered, the customer is expected to perform the following measures:

a) Receive the package.

b) Acknowledge received items receipt

33 FNS personnel will keep the Acknowledge received items as proof of product receipt. Customer is expected to use “Guardian - CCS Blockchain Security Authentication (BSA) Web Application Integration” for web application integration if required. Acceptance of product will be based on customer’s selection of product functionalities

2 Evaluation

34 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 5 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 5 (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

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

2.1.1 Life-cycle support

36 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.

37 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

38 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).

39 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.

40 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.

41 At the end, the evaluators confirmed that all the requirements for this class were fulfilled and passed.

2.1.3 Guidance documents

42 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.

43 The evaluators confirmed that the TOE guidance was fulfilled all the requirements and passed for this class.

2.1.4 IT Product Testing

44 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by Cybertronics Lab. 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

45 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

46 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.

47 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.

Table 3: Functional Test

Test ID	Justification	Description	Security Function	Results
FT001	To ensure user's_ able to successfully on-board to BSA application.	This SFR specify that user is allowed to perform onboarding through mobile application and register the mobile device	FIA_ATD.1 User Attributes Definition FDP_ACF.1 Security Attribute-Based Access Control	Passed
FT002	To ensure user able to authenticate through BSA and login into web portal.	This SFR specify that the user can perform authentication to login into the application through TOE.	FIA_ATD.1 User Attributes Definition FDP_ACF.1 Security Attribute-Based Access Control	Passed
FT003	To ensure BSA mobile application calls to BSA API to request and retrieve the authentication token during the authentication process.	This SFR specify that the TOE will assign a unique token during each authentication process.	FIA_UAU.2 User Authentication Before Any Action FIA_UID.2 User Identification Before Any Action	Passed

Test ID	Justification	Description	Security Function	Results
FT004	To ensure FNS Manager user role able to authenticate through BSA and login into web portal.	This SFR specify that each user will have privilege to access and use web portal functions-based roles	FDP_ACC.1 Subset Access Control FMT_SMF.1 Specification of Management Functions	Passed
FT005	To ensure Vendor Manager user role able to authenticate through BSA and login into web portal.	This SFR specify that each user will have privilege to access and use web portal functions-based roles	FDP_ACC.1 Subset Access Control FMT_SMF.1 Specification of Management Functions	Passed
FT006	To ensure Client Manager user role able to authenticate through BSA and login into web portal.	This SFR specify that each user will have privilege to access and use web portal functions-based roles	FDP_ACC.1 Subset Access Control FMT_SMF.1 Specification of Management Functions	Passed
FT007	To ensure Normal user role able to authenticate through BSA and login into web portal.	This SFR specify that each user will have privilege to access and use web portal functions-based roles	FDP_ACC.1 Subset Access Control FMT_SMF.1 Specification of Management Functions	Passed
FT008	To allow the user to identify previous authentication history.	This SFR allow users to review past successful and unsuccessful attempt of authentication on linked application	FTA_TAH.1 TOE Access History	Passed

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

2.1.4.3 Vulnerability Analysis

49 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, and security architecture description.

50 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 and Enhanced 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

51 The penetration tests focused on:

a) Broken Object Level Authorization

b) Broken User Authentication

c) Excessive Data Exposure

d) Lack of Resources & Rate Limiting

e) Broken Function Level Authorization

f) Security Misconfiguration

g) Injection

h) Improper Assets Management

52 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

53 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

54 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24 which is performed by Cybertronics Lab.

55 Cybertronics Lab found that Guardian-CCS Blockchain Secure Authentication (BSA) v1.0.24 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.

56 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. The risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

57 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.

58 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.

59 EAL 2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

60 The Malaysian Certification Body (MyCB) is strongly recommended that:

a) A strict adherence to the guidance documentations and procedures provided by the developer.

b) The TOE users should aware and implement available security or critical updates related to the TOE security features and its supporting hardware, software, firmware or relevant guidance documents.

c) Users are advice to seek assistance or guidance directly from the developer of the TOE if specific requirements need to be configured or implemented on the TOE to meet certain policies, procedures or security enforcement within the users' organization. This is important to reduce operational error, misconfiguration, malfunctions and insecure operations of the TOE that may compromise the confidentiality, integrity and availability of the assets that is protected by the TOE.

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 3.1, Revision 5, April 2017.

[3] The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017.

[4] MyCC Scheme Requirement (MYCC_REQ), v1, CyberSecurity Malaysia, December 2019.

[5] ISCB Evaluation Facility Manual (ISCB_EFM), v2a, August 2020.

[6] Guardian-CCS Blockchain Secure Authentication (BSA) Security Target, Version 1.2, 29 August 2022.

[7] AVCC008 Evaluation Technical Report (ETR) Version 1.1, 5 August 2022.

A.2 Terminology

A.2.1 Acronyms

Table 4: 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
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

Acronym	Expanded Term
TOE	Target of Evaluation
FSP	Functional Specification
TDS	TOE Design
SFR	Security Functional Requirement
TSF	TOE Security Function

A.2.2 Glossary of Terms

Table 5: 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-today 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
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.

Term	Definition and Source
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 ---