MINISTRY OF DIGITAL

CyberSecurity MALAYSIA

C141 Certification Report

Meja Bulat Version 5.15.3

File name: ISCB-5-RPT-C141-CR-v1
Version: v1
Date of document: 13 March 2026
Document classification : PUBLIC

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

C141 Certification Report

Meja Bulat Version 5.15.3

13 March 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:	C141 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C141-CR-v1
ISSUE:	v1
DATE:	13 March 2026
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. 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 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).

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 Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, November 2022 (Ref [3]), for conformance to the Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, November 2022 (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	3 February 2026	All	Initial draft
d2	24 February 2026	viii, 3, 9	Based on Senior Certifier and Scheme Manager comments during internal review process, several updates are required including amendments to the Final ETR v1.0. The changes of these documents are: i) Added project code, developer name and update completion evaluation date ii) Added Common Criteria Errata and Interpretation for CC:2022 under Methodology in Table 1 iii) Section 2.1.4.2 update title to Independent Functional Testing
d2a	3 March 2026	iv, viii	i) Amendments of the sentences on certification details will be updated on ISCB and CCRA website. ii) Added information regarding potential user and certification validity.
v1	13 March 2026	All	Final version

Executive Summary

The project is C141 Meja Bulat Version 5.15.3, referred to as the Target of Evaluation (TOE) which developed by Infosys Gateway Sdn Bhd.The TOE is a web application that is designed as a secure meeting platform that provides protected end to end encryption and protected environment for individuals and organizations to conduct virtual meetings, conferences, and collaborations.

The TOE offers end-to-end encryption that ensures the content of a virtual meeting, such as audio, video, and chat messages, is encrypted at the source and can only be decrypted by the intended participants, providing a high level of security and privacy for the meeting's communications.

End-to-end encryption, one of the hallmark elements, ensures that the content exchanged during a meeting remains private and secure. This means that only authorized participants possess the decryption keys, rendering the data inaccessible to potential eavesdroppers, including the platform provider.

The TOE provides security functions such as secure communication, cryptographic support, identification and authentication, and security management.

The scope of the evaluation is defined by the Security Target (Ref[7]) 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. Users are advised to review the intended operating environment and confirm that the stated security objectives can be effectively met by considering 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 1 (EAL1). 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 [5]).

The evaluation was performed by Securelytics SEF and the evaluation was completed on 19 February 2026.

This Certification Report is associated with the Certificate of Product Evaluation dated 24 Mar 2026 and the Security Target (Ref[7]). 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 Meja Bulat Version 5.15.3 meets their specific requirements. Potential users of the TOE are advised to refer to the Security Target (Ref[7]) and this Certification Report prior making a purchase decision.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE) is Meja Bulat Version 5.15.3 is a web application that is designed as a secure meeting platform and provides environment for individuals and organizations to conduct virtual meetings, conferences and collaborations.

2 This platform prioritizes the safeguarding of sensitive information and privacy, offering a range of robust security features.

3 The TOE offers end-to-end encryption that ensures the content of a virtual meeting, such as audio, video, and chat messages, is encrypted at the source and can only be decrypted by the intended participants, providing a high level of security and privacy for the meeting's communications.

4 End-to- end encryption, one of the hallmark elements, ensures that the content exchanged during a meeting remains private and secure. This means that only authorized participants possess the decryption keys, rendering the data inaccessible to potential eavesdroppers, including the platform provider.

5 Additionally, user authentication, access controls, and password protection help prevent unauthorized access, guaranteeing that only invited participants can join the meeting. Furthermore, regular updates and compliance with industry regulations ensure that secure online meeting platforms stay ahead of emerging threats, making them a vital resource for organizations aiming to collaborate safely in a digital world.

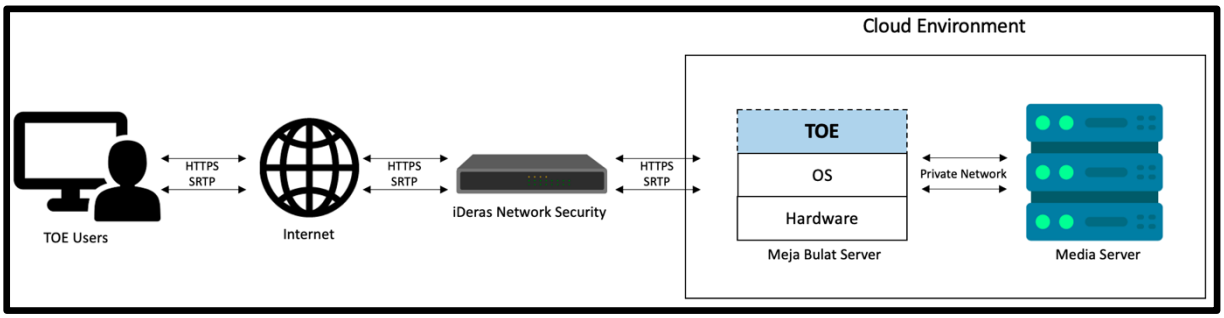
6 The TOE offers a variety of features to facilitate effective communication and collaboration. Here is a list of common features:

- Video Conferencing: Support for video calls with multiple participants, including the ability to see and interact with each other through webcams.
- Audio Conferencing: High-quality audio calls, often with features like noise cancellation and the ability to mute/unmute participants.
- Screen Sharing: Share your screen with others to showcase presentations, documents, or software applications.
- Chat and Messaging: Real-time text chat for participants to exchange messages during the meeting.
- Recording: The ability to record meetings for later reference or sharing with absent participants.

- Virtual Backgrounds: The option to use virtual backgrounds or blur the background for privacy.
- Hand Raise and Reactions: Features that allow participants to signal when they want to speak or show agreement/disagreement.
- Participant Management: Hosts can mute/unmute participants, remove disruptive users, or manage permissions.

7 The TOE is designed with various security features and protocols to protect against unauthorized access, eavesdropping, data breaches, and other security threats.

8 Figure 1 shows blue box is the scope of the TOE. To perform the TOE operation, the TOE will need to communicate with several servers that are hosted locally in the developer environment which is located in Malaysia which are Meja Bulat Server and Media Server. The description for physical and logical boundary is provided in Section 1.4 in this document.



Legend:

TOE Boundary

Figure 1: TOE

1.2 TOE Identification

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

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C141
TOE Name	Meja Bulat
TOE Version	5.15.3
Security Target Title	Meja Bulat Version 5.15.3 Security Target
Security Target Version	v1.1
Security Target Date	24 Jan 2026
Assurance Level	Evaluation Assurance Level 1
Criteria	Common Criteria for Information Technology Security Evaluation, CC:2022, Revision 1, November 2022 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, CC:2022, Revision 1, November 2022 (Ref [3]) Common Criteria Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, July 22, 2024 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL 1
Sponsor	Infosys Gateway Sdn Bhd Suite 3.02B, Level 3, South Wing, Menara OBYU, No.4 Jalan PJU 8/8A, Damansara Perdana, 47820 Petaling Jaya Selangor, Malaysia
Developer	Infosys Gateway Sdn Bhd Suite 3.02B, Level 3, South Wing, Menara OBYU, No.4 Jalan PJU 8/8A, Damansara Perdana, 47820 Petaling Jaya Selangor, Malaysia
Evaluation Facility	Securelytics SEF

	A-17-01, Tower A, Atria Sofo Suites, Jalan SS 22/23, Damansara Utama, 47400 Petaling Jaya, Selangor, Malaysia

Table 1: TOE Identification

1.3 Security Policy

10 No Organisational Security Policy declared for the TOE.

1.4 TOE Architecture

11 The TOE consist of logical and physical boundaries which are described in Section 1.4 of the Security Target (Ref[7]).

1.4.1 Logical Boundaries

- **Secure Communication**
  The TOE provides a secure communication between the TOE and servers by utilizing HTTPS (TLS v1.2) and SRTP (AES-GCM-256).
- **Cryptographic Support**
  The TOE implements encryption algorithm that utilizes AES-GCM-256.
- **Identification and Authentication**
  All users must be identified and authenticated before any information is permitted to flow. There are two types of users: TOE User and TOE Moderator. There are several login options on the login page:
  - Login using personal email: TOE Users need to input their personal email.
  - Login using Google account: TOE Users can sign in using their Google account.
  - Login using Spotify account: TOE Users can access the TOE through their Spotify account.
  - Login using X account: TOE Users can log in using their X account.
  - Login as TOE moderator: The System Administrator registers the TOE user as a TOE moderator.
- **Security Management**

The TOE contains various management functions to ensure efficient and secure management of the TOE users. The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The TOE provides a web-based interface that permits the TOE moderator user to manage the virtual meeting.

1.4.2 Physical Boundaries

12 The TOE is a web application and is used by the TOE users and TOE moderator to perform operations.

13 The primary access to the TOE is via web application GUI by browsing to a link provided by the developer which is https://secure.infosysgateway.com.my.

14 In order to perform the TOE operation, the TOE will need to communicate with several servers that are hosted in the developer environment which is located in Malaysia:

i) Meja Bulat Server: Web Server is a server to host the TOE web application and system management console. System management console is a web based system used by the System Administrator to manage the TOE Moderators and TOE users. Note that System Administrator and system management console are out of the scope of evaluation

ii) Media Server: The Media Server is a PC that utilizes an Intel GPU and is connected to the internet via an Ethernet cable, which is also known as Ethernet Intel. The PC used for standby media server purposes is out of the scope of testing. This ready media server will act as a host if the TOE moderator who wants to host the meeting does not meet the media server requirement. Note that Media Server is out of the scope of evaluation.

1.5 Clarification of Scope

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

16 Figure 1 and Section 1.4 of this document describe the scope of the evaluation, which is limited to those claims made in the Security Target (Ref[7]).

17 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

Identifier	Assumption statement
A.AUTHORISE	The TOE user and TOE moderator are not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by the developer
A.OPSYS	The operating systems hosting the TOE components safeguard them from unauthorized access, modification, or deletion.
A.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE.
A.OS	The OS platforms on which the TOE operates is hardened to counter the perceived threats.
A.TIMESTAMP	The platforms on which the TOE operates provides reliable timestamps.
A.CRED	The TOE Moderator and TOE User will take appropriate measures to safeguard credentials employed for third-party authentication (such as X, Google, or Spotify), ensuring they are protected against potential threats and not exposed to unauthorized users.

1.7 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.

19 The TOE was installed and operated on the following server configuration (minimum requirement)

- Operating System: Ubuntu 22.04 LTS
- Processor: 8 vCPUs
- Memory: 16 GB RAM
- Storage: 1TB
- Database: PostgreSQL 12
- Supporting software: Docker (web hosting environment)

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

- Operating System: Windows 10
- Processor: 11th Gen Intel® Core™ i7-1165G7 @ 2.80 GHz
- Memory: 8 GB RAM
- Web Browsers:
  - Google Chrome version 134
  - Mozilla Firefox version 136
  - Microsoft Edge version 134

21 The TOE was evaluated with the following cryptographic mechanisms enabled:

- TLS v1.2 to provide trusted communication paths between the TOE and users
- SRTP using AES-GCM-256 to protect media communication

These cryptographic mechanisms support the security functional requirements defined in the ST, including secure communication and cryptographic operations.

2 Evaluation

22 The evaluation was conducted in accordance with the requirements of the Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, November 2022 (Ref [2]) and Common Methodology for Information Technology Security Evaluation, Evaluation methodology CC:2022 Revision 1, November 2022 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). The evaluation was performed conformant to the MyCC Scheme Requirement (MyCC_REQ) (Ref [5]) and ISCB Evaluation Facility Manual (ISCB_EFM) (Ref [6]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

24 The evaluator found that the TOE provided for evaluation is labelled with its reference.

25 The evaluator check that the TOE references used are consistent.

26 The evaluator examine the configuration list to determine that it uniquely identifies each configuration item.

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

2.1.2 Development

28 The functional specification shall describe the purpose and method of use for use for each SFR-enforcing and SFR-supporting TSFI.

29 The evaluator examined the presentation of the TSFI to determine that it identifies all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

30 The evaluator examined the rationale provided by the developer for the implicit categorization of interfaces as SFR non-interfering to determine that it is accurate.

31 The evaluator shall examine the functional specification to determine that it is a complete instantiation of the SFRs.

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

2.1.3 Guidance documents

33 The evaluator 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.

34 The evaluator examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

35 TOE user may refer Meja Bulat V5.15.3 Quick Guide as guidance documentation.

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

2.1.4 IT Product Testing

37 Testing at EAL1 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

38 The evaluators verified that the developer has met their testing responsibilities by repeating some developer test, as documented in the Evaluation Technical Report (Ref[8]) (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

39 At EAL1, provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

40 An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.

Test ID	Descriptions	Security Functional Requirement (SFR)	Results
F001-Cryptographic Operation	To test that the TOE generate cryptographic keys in accordance with a specified cryptographic key generation algorithm; ECDSA, AES-CM-256-HMAC-SHA1-80 and specified cryptographic key sizes; ECDSA (256-bit keys), AES-CM-256-HMAC-SHA1-80 (256-bit keys) that meets; ECDSA (FIPS186-4), AES-CM-256-HMAC-SHA1-80 (FIPS197).	FCS_CKM.1.1, FCS_COP.1.1	PASS
F001-Cryptographic Operation	To test that the TOE destroy cryptographic keys in accordance with a specified cryptographic key destruction method; key zeroization.	FCS_CKM.4.1	PASS
F003 – Identification and Authentication	To test that the TOE maintain the following list of security attributes belonging to individual users: · Username/Email · Password	FIA_ATD.1.1	PASS
F004 – 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 authenticated and identified before allowing any other TSF-mediated actions on behalf of that user.	FIA_UAU.2.1, FIA_UID.2.1	PASS
F005–Security Management	1. To test that the TOE Moderator is able to log in using the login interface.	FMT_SMF.1.1	PASS

	2. To test that the TOE Moderator is able to manage audio settings including mute/unmute, viewing or editing microphone settings, and viewing or editing speaker settings. 3. To test that the TOE Moderator is able to control video settings including start/stop camera, view or edit the camera, view or edit virtual background, and edit video mirroring. 4. To test that the TOE Moderator is able to initiate screen sharing. 5. To test that the TOE Moderator is able to open and close the chat window. 6. To test that the TOE Moderator is able to raise or lower their hand. 7. To test that the TOE Moderator is able to manage participants by inviting or searching for participants, muting all, disabling all cameras, granting moderator rights, kicking out participants, sending private messages, and adding breakout rooms. 8. To test that the TOE Moderator is able to access more actions including inviting people, viewing or editing performance, viewing full screen, viewing or editing security options, starting a recording, sharing video, enabling or disabling noise suppression, showing or hiding the whiteboard, and viewing participants' statistics. 9. To test that the TOE User is able to log in using the login interface. 10. To test that the TOE User is able to manage audio settings including		

	mute/unmute, viewing or editing microphone settings, and viewing or editing speaker settings. 11. To test that the TOE User is able to control video settings including start/stop camera, view or edit the camera, view or edit virtual background, and edit video mirroring. 12. To test that the TOE User is able to initiate screen sharing. 13. To test that the TOE User is able to open and close the chat window. 14. To test that the TOE User is able to raise or lower their hand. 15. To test that the TOE User is able to manage participants by inviting or searching for participants and sending private messages. 16. To test that the TOE User is able to perform additional actions including inviting people, viewing or editing performance, viewing full screen, starting a recording, sharing video, enabling or disabling noise suppression, showing or hiding the whiteboard, viewing participants' statistics, and viewing or editing settings.		
F006- Security Management	1. To test that the TOE maintain the roles of TOE User and TOE Moderator. 2. To test that the TOE are able to associate users with roles.	FMT_SMR.1.1, FMT_SMR.1.2	PASS
F007–Secure Communication	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	FTP_TRP.1.1, FTP_TRP.1.2, FTP_TRP.1.3	PASS

	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.		

Table 2: Independent Functional Test

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.

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, 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) Cryptographic Failures

c) Injection

d) Insecure Design

e) Security Misconfiguration

f) Vulnerable and Outdated Components

g) Identification and Authentication Failures

h) Software and Data Integrity Failures

i) Security Logging and Monitoring Failures

j) Server-Side Request Forgery (SSRF)

46 Considering as Basic attack potential no identified vulnerabilities are exploitable. However, identified residual vulnerabilities require a higher attack potential. These vulnerabilities are acceptable within the scope and limitations of the claimed Evaluation Assurance Level (EAL1) and do not adversely affect the achievement of the TOE security objectives as defined in the Security Target (Ref[7]). Accordingly, these residual vulnerabilities do not preclude certification. The residual vulnerabilities are given below:

Test ID: P004 Vulnerability Method: Insecure Design-Input Validation

Test ID: P009 Vulnerability Method: Security Logging & Monitoring Failures-No Account Lockout

Both Attack Calculation: 11(**Enhanced-Basic**)

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 of the Evaluation Technical Report (Ref [8]), the Malaysian Common Criteria Certification Body certifies the evaluation of Meja Bulat Version 5.15.3 which is performed by Securelytics SEF.

49 Securelytics SEF found that Meja Bulat Version 5.15.3 upholds the claims made in the Security Target (Ref[7]) and supporting documentations, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 1(EAL1).

50 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

51 EAL1 provides a basic level of assurance by a limited security target and analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.

52 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TSF.

53 EAL1 also provides assurance through unique identification of the TOE and the relevant evaluation documents.

54 This EAL provides a meaningful increase in assurance over unevaluated IT.

3.2 Recommendation

55 The Malaysian Certification Body (MyCB) is strongly recommended (Opinions and interpretations expressed herein are outside the scope of certification) that:

i) TOE users should check their operational environment can support the security functional requirements defined for the TOE.

ii) TOE users should read and follow all guidance provided by the developer, especially any security warnings.

iii) TOE users and TOE developer should protect any security-related data used during initialization, start-up, and operation, especially when it is handled outside the TOE.

iv) TOE users should review TOE's audit logs regularly.

v) TOE developer should ensure the TOE is physically protected, restrict access to internal parts, and verify tamper-evident bag serial numbers upon delivery.

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] Common Criteria for Information Technology Security Evaluation, CC:2022 Revision 1, November 2022.

[3] Common Methodology for Information Technology Security Evaluation, Evaluation methodology CC:2022 Revision 1, November 2022.

[4] Common Criteria Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1), Version 1.1, July 22, 2024

[5] MyCC Scheme Requirement (MYCC_REQ), V2, 24 April 2025.

[6] ISCB Evaluation Facility Manual (ISCB_EFM), V3, 24 April 2025.

[7] Meja Bulat Version 5.15.3 Security Target, v1.1, 24 Jan 2026.

[8] Evaluation Technical Report–Meja Bulat Version 5.15.3 (T2305-2-ETR 1.1), 19 February 2026.

A.2 Terminology

A.2.1 Acronyms

Table 3: 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

Acronym	Expanded Term
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
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: 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.

Term	Definition and Source
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.
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 ---