MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

C106 Certification Report

LGMS Security Assessment Report Generator (LGMS Reporter) v 1.0.0

File name: ISCB-5-RPT-C106-CR-V1
Version: v1
Date of document: 19 December 2019
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

Securing Our Cyberspace

C106 Certification Report

LGMS Security Assessment Report Generator (LGMS Reporter) v 1.0.0

19 December 2019

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:	C106 Certification Report
DOCUMENT REFERENCE:	ISCB-5-RPT-C106-CR-V1
ISSUE:	v1
DATE:	19 December 2019

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. 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 24 December 2019, 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).

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 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	16 December 2019	All	Initial draft
d2	18 December 2019	All	Review and amend by Senior Certifier
v1	19 December 2019	All	Final Version

Executive Summary

The Target of Evaluation (TOE) is a web-based report generator which provides the service through Internet. TOE helps to simplify users experience as a one-stop presentation medium that displays the vulnerability assessment results in report.

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 LGMS Infosec Lab Sdn Bhd and the evaluation was completed on 3 December 2019.

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 LGMS Security Assessment Report Generator (LGMS Reporter) v1.0.0 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) is a web-based report generator which provides the service through Internet. TOE helps to simplify users experience as a one-stop presentation medium that displays the vulnerability assessment results in report. The software application is installed in a dedicated virtual machine. The physical server that hosts the virtual machine is managed by LE Global Services Sdn Bhd. The platform, virtual machine and SQL database of the TOE are out of scope. Users are able to access to TOE upon successful authentication through web browser and perform the operations. There is no installation required in order to access to the functions of the TOE. Physical scope is not applicable for this TOE.

2 The TOE provides the following security features:

- Identification and Authentication
- Security Audit Logs
- Trusted Path/Channels
- User Data Protection
- Security Management

1.2 TOE Identification

3 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C106
TOE Name	LGMS Security Assessment Report Generator (LGMS Reporter)
TOE Version	V1.0.0
Security Target Title	LGMS Security Assessment Report Generator Security Target
Security Target Version	V2.0
Security Target Date	10 December 2019
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	LE Global Services Sdn Bhd
Developer	LE Global Services Sdn Bhd
Evaluation Facility	LGMS Infosec Lab Sdn Bhd

1.3 Security Policy

4 There is no organisational security policy defined regarding the use of TOE.

1.4 TOE Architecture (ADV_ARC)

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

1.4.1 Logical Boundaries

6 The TOE provides the feature for user to upload raw results from different vulnerability scanners, process the raw data and provide consolidated results. The TOE can only be used by the authenticated user via web browser. User will need to obtain the account username and password from administrator in order to use the TOE.

Table 2: LGMS Reporter Security Features

Identification and Authentication	TOE will identify and authenticate the user before any actions can be performed. Unauthorized attempt will be recorded in the audit log.
Security Audit Logs	TOE will generate audit logs for auditable events. These audit records can only be accessed by the TOE administrator.
Trusted Path/Channels	TOE provides the secure channel communication (HTTPS) between the TOE and TOE user.
User Data Protection	TOE provides the feature to protect user data based on the role-based access control matrix and second layer authentication when generating the report.
Security Management	TOE allows authenticated user to manage their own password. TOE administrator will be able to manage the user account such as update user's role and reset user's password.

1.4.2 Physical Boundaries

7 Physical scope is not applicable for this TOE.

1.5 Clarification of Scope

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

9 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]).

10 Potential consumers of the TOE are advised that some functions and services of the overall product have not have 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

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

1.6.1 Environmental assumptions

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

Table 3: Assumptions for the TOE environment

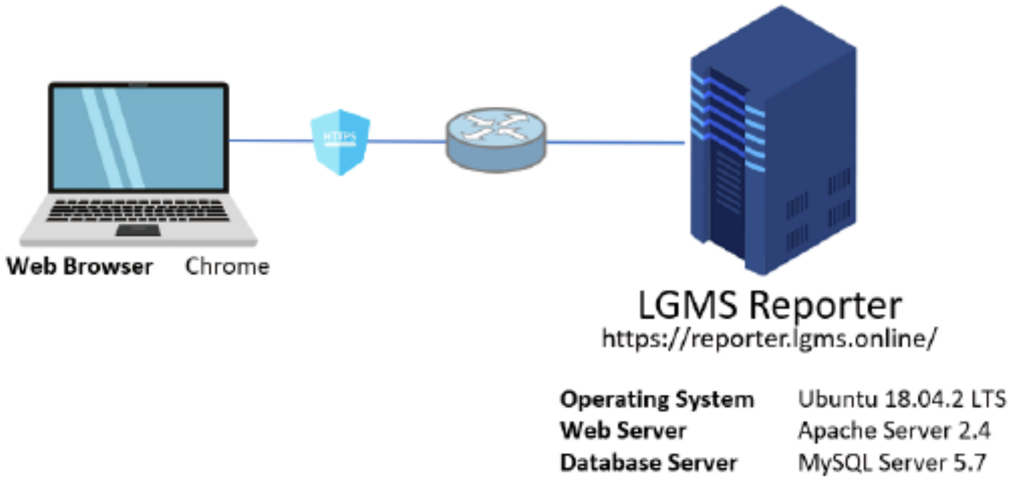
Assumption	Statements
A.PHY	It is assumed that the TOE and its platform are located within secured facilities with controlled access to prevent unauthorized physical access.
A.TIMESTAMP	It is assumed that the TOE operational environment is able to provide reliable timestamp for TOE which will affect the time accuracy of audit logs.
A.ADMIN	It is assumed that authorized TOE administrators have no malicious intention; and are appropriately trained to undertake the configuration and management of the TOE

1.7 Evaluated Configuration

13 LGMS Reporter may be deployed in a number of configurations consistent with the requirements identified in this Security Target (Ref [6]). Where the deployed environment satisfies the objectives stated in 6.2 in Security Target (Ref [6]).

14 LGMS Reporter deployment is using Ubuntu as host operating system and running in web server. The deployment is illustrated in Figure 1 below.

Figure 1: Example LGMS Reporter Deployment


Web Browser
Chrome
LGMS Reporter
https://reporter.lgms.online/
Operating System Ubuntu 18.04.2 LTS
Web Server Apache Server 2.4
Database Server MySQL Server 5.7

15 The evaluator has verified that the TOE samples are provided in the above-described state.

1.8 Delivery Procedures

16 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.

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

1.8.1 TOE Delivery Procedures

18 In order to access the TOE, TOE user requires to request an account from the TOE administrator through email address (reporter@lgms.online) with the account request form. The account request form can be downloaded from https://reporter.lgms.online/document/2019 LGMS Security Assessment Report Generator Account Request Form-v1.0.pdf.

19 Steps to obtain an account are as follow:

1. User should download and fill in the user account request form.
2. Then send an email to request for account creation with the the form as attachment to TOE administrator at reporter@lgms.online.
3. Once the details are verified, TOE administrator will create the account and send the information and instruction through email to the TOE user.

4. TOE user is advised to follow the instructions in the email to access the TOE.

20 Users will be informed if there is any new update or changes from the TOE through the registered email address. It is advised to validate the updated TOE version from the site footer are same as the updated version informed through email. Besides, is recommended to clear browser cache before accessing the updated TOE web application.

2 Evaluation

21 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

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

2.1.1 Life-cycle support

23 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.

24 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

25 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).

26 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.

27 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.

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

2.1.3 Guidance documents

29 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.

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

2.1.4 IT Product Testing

31 Testing at EAL 2 consists of assessing developer tests, performing independent functional test, and conducting penetration tests. The TOE testing was conducted by LGMS Infosec Lab Sdn Bhd. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Report.

2.1.4.1 Assessment of Developer Tests

32 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

33 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.

34 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 4: Independent Functional Test

Test Suite	Description	Results
Test-ATE-001	• Conduct test case ID SECMANAGE-002 specified in the developer's test documents to validate developer's test result. • The TOE shall allow the login of the newly created account and redirect the user to home page when successful login.	Passed. Result as expected.
Test-ATE-002	• Conduct test case ID IAA-001 specified in the developer's test documents to validate developer's test result. • The TOE shall reject the login attempt with the proper error message after 5 failure login attempts. • The TOE shall reject the login until the account has been unlocked automatically after 30 minutes of lock period or manually unlocked by administrator.	Passed. Result as expected.

Test Suite	Description	Results
Test-ATE-003	• Conduct test case SECMANAGE-004 specified in the developer's test documents to validate developer's test result. • The TOE shall allow user with administrator role to reset the user password with new password. • The TOE shall allow the login of the account with new password and redirect to home page if the username and new password provided are correct.	Passed. Result as expected.
Test-ATE-004	• Conduct test case ID IAA-002 specified in the developer's test documents to validate developer's test result. • The TOE shall reject the user creation request and prompt "Password strength does not meet requirement."	Passed. Result as expected.
Test-ATE-005	• Conduct test case ID AUDIT-001 specified in the developer's test documents to validate developer's test result. • The TOE shall record the required logs for the appropriate events.	Passed. Result as expected.
Test-ATE-006	• Conduct test case ID UDP-001 specified in the developer's test documents to validate developer's test result. • The TOE shall prompt "No results found." message if the data does not belong to the rightful owner.	Passed. Result as expected.

Test Suite	Description	Results
Test-ATE-007	• Conduct independent test to identify inactive account login ability. • The TOE shall prompt login failed message.	Passed. Result as expected.

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

2.1.4.3 Penetration testing

36 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.

37 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) Any public knowledge of the vulnerability or known exploit;

b) The complexity of the vulnerability and its identification;

c) The exploitability of the identified vulnerability;

d) The time required to perform the exploit of vulnerability;

e) Level of knowledge towards the TOE; and

f) Additional resource(s), if any, required for an exploitation

38 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 Section 4 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

39 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

40 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref), the Malaysian Common Criteria Certification Body certifies the evaluation of LGMS Security Assessment Report Generator (LGMS Reporter) v 1.0.0 which is performed by LGMS Infosec Lab Sdn Bhd.

41 LGMS Infosec Lab Sdn Bhd found that LGMS Security Assessment Report Generator (LGMS Reporter) v 1.0.0 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.

42 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

43 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.

44 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.

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

3.2 Recommendation

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

a) The potential consumer of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed in Security Target (Ref [6]).

b) The System Administrator should review the audit trail generated and exported by the TOE periodically.

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), v2, December 2019.

[6] LGMS Security Assessment Report Generator Security Target, Version 2.0, 10 December 2019.

[7] Report Generator (Reporter) Evaluation Technical Report, Version 2.0, 10 December 2019.

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-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

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 ---