C056 Certification Report

d'COMPASS v2.0.0

File name: ISCB-5-RPT-C056-CR-v1
Version: v1
Date of document: 24 December 2014
Document classification: PUBLIC

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

C056 Certification Report

d'COMPASS v2.0.0

24 December 2014
ISCB Department

CyberSecurity Malaysia
Level 5, Sapura@Mines,
No 7 Jalan Tasik,The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8992 6888 Fax: +603 8992 6841
http://www.cybersecurity.my

Copyright Statement

Registered office:
Level 5, Sapura@Mines
No 7, Jalan Tasik,
The Mines Resort City,
43300 Seri Kembangan
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 2014, 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 at www.commoncriteriaportal.org).

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 (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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	9 December 2014	All	Initial draft.
d2	15 December 2014	ix of x, 3/14	Update table of content, details of logical boundaries and change the date.

Executive Summary

d'COMPASS v2.0.0 from TriAset Sdn Bhd is the Target of Evaluation (TOE) for the Evaluation Assurance Level 2 (EAL2) evaluation.

d'COMPASS is web application designed to be used as a Treasury Management System for a web-based application environment. The TOE provides security functionality such as access control, identification and authentication, security management and secure communication.

TOE features include:

a) Single point of entry for every trade

b) Centralised risk and compliance controls

c) Centralised information in a global data repository

d) Flexibility to incorporate new processes and external and reports

e) Wide range user-defined intelligent enquiries and reports

f) Ease of connection with external applications and tools.

The scope of evaluation covers major security features as follow:

a) Access control- the TOE manages access control within each organisation based on user Ids, user roles and access control lists. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

b) Identification and Authentication- the TOE requires that each user is successfully identified (user Ids) and authenticated (password) before any interaction with protected resources is permitted.

c) Secure Management- the TOE provides functions that allow management of the TOE and its security functions. The TPOR restricts access to the management functions based on the role of the user.

d) Security Communication- the TOE is able to protect the user data from disclosure and modification using SSL as a secure communication between users' browser and the TOE.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for TOE, the security function 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 MySEF CyberSecurity Malaysia evaluation facility and completed on 3 December 2014.

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 www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of user to ensure that d'COMPASS meet their requirements. It is recommended that a potential user of d'COMPASS to 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

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), d'COMPASS v2.0.0 (hereafter referred as d'COMPASS) is an online Treasury Management System that caters for managing and operating treasury, financial asset investment and financial risks.

2 The TOE provides a complete solution from back to the front office fund management operation.

3 The TOE is a web application that is developed entirely from Java-based technologies which is installed into a Java EE-compliant application server and accessible via a web browser.

4 The TOE primary features include:

a) Single point of entry for every trade

b) Centralised risk and compliance controls

c) Centralised information in a global data repository

d) Flexibility to incorporate new process and external data flows

e) Wide range user-defined intelligent enquiries and reports; and

f) Ease of connection with external applications and tools.

5 The major security functions that implemented by the TOE are as below:

a) **Access control**- the TOE manages access control within each organisation based on user Ids, user roles and access control lists. Each ACL maps users and roles to the operations that they are permitted to perform on the object.

b) **Identification and Authentication**- the TOE requires that each user is successfully identified (user IDs) and authenticated (password) before any interaction with protected resources is permitted.

c) **Security Management**- the TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.

d) **Security Communication**- the TOE is able to protect the user data from disclosure and modification using SSL as a secure communication between users' browser and the TOE.

1.2 TOE Identification

6 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	C056
TOE Name	d’COMPASS
TOE Version	2.0.0
Security Target Title	d’COMPASS Security Target
Security Target Version	Version 1.0
Security Target Date	1 October 2014
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2
Sponsor and Developer	TriAset Sdn Bhd Unit 23-5, 5th Floor Block E1, Jalan PJU 1/42 Dataran Prima, 47301 Petaling Jaya, Selangor
Evaluation Facility	CyberSecurity Malaysia MySEF (CSM MySEF)

1.3 Security Policy

7 There are no organisational security policies have been defined regarding the use of the TOE.

1.4 TOE Architecture

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

1.4.1 Logical Boundaries

9 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) **Access Control**

The TOE enforces an access control policy on protected resources. After a user is identified and authenticated to the TOE, the TOE will check all HTTP request from the user to the protected resource. The TOE will permit a user to access a protected resource (FDP_ACC.1, FDP_ACF.1). The TOE maintains access control list (ACL) for each object within an organisation. Each ACL maps users and roles to the operations that they are permitted to perform on the object. There 2 users roles maintained by the TOE. They are users and systems admin (**FMT_SMR.1**). Each type of user will have different access rights to a protected resource. All users will have a unique user ID.

b) **Identification and Authentication**

When a user issues a request to the TOE to access a protected resource (methods or HTML pages), the TOE requires that the user (Users and System Admins) identify and authenticate themselves before performing any TSF mediated action (FIA_UID.2, FIA_UAU.2). The TOE will compare the credentials by checking the information presented by the user at the login page against the authentication information stored in the database. All user presented passwords are hashed before being used to authenticate to the TOE, or when users change their passwords (FMT_MTD.1b) to be written to the database. This is all done by the TOE (FCS_COP.1).

c) **Security Management**

The TOE contains various management functions to ensure the efficiency and security management of the TOE (FMT_SMF.1):

The role of the system admin can modify the access control list and mapping of users to roles (FMT_MSA.1). The TOE provides a suite of management functions to system admin and users which thee functions allow for the configurations of the TOE to suit the organization in which it is deployed. Moreover, management roles may perform the following task;

- assign user Ids to roles
- add, delete and edit user Ids and roles
- delete, edit and view operation functions;
- cancelling of form changes
- closing the form
- changing of password, and
- security setting

System admin may assign and adjust the functions available to users; users may assign and adjust the functions based on organization's requirement(s) (FMT_SMR.1 and FMT_MTD.1a).

d) **Security Communications**

When a user accesses to the TOE on their browser by typing in the website address, the TOE will initiate a SSL secure channel establishment with the user's browser (FTP_TRP.1). The TOE implements the Secure Sockets Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols.

1.4.2 Physical Boundaries

10 The TOE is a web application (Java-based) for Treasury Management System hosted on the server. A typical installation of the TOE can be found in Figure 1 below, which identifies the various components of the TOE architecture.

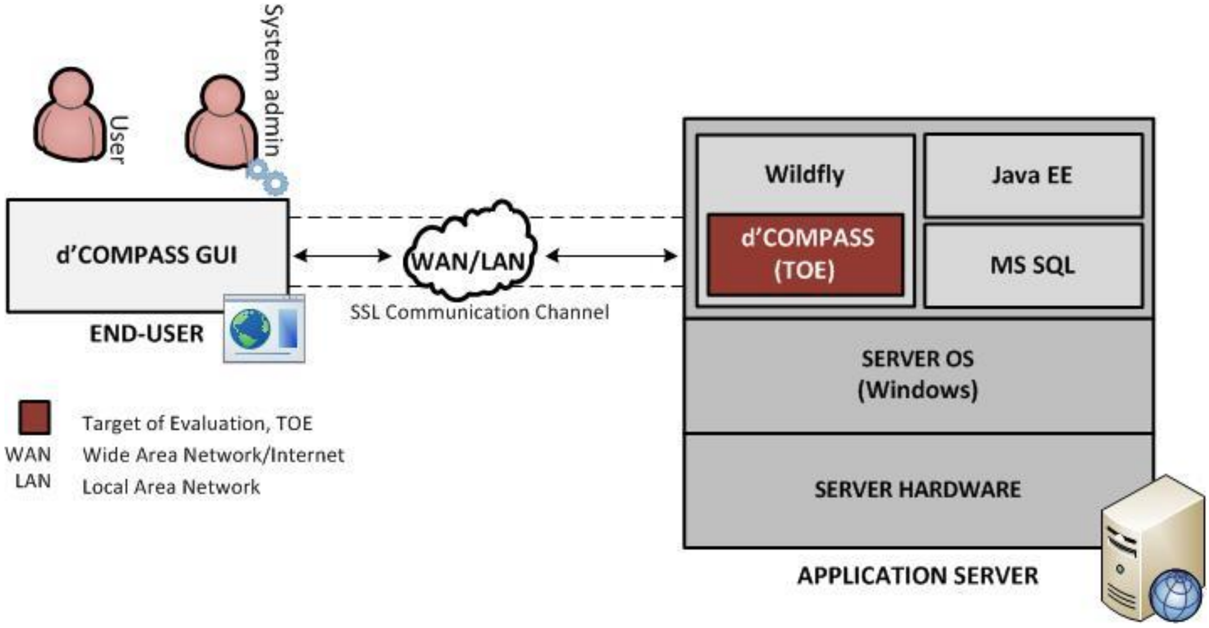

Figure 1: TOE Overview

11 The TOE Graphic User Interface (GUI) is installed on the dedicated host server for user to perform management of the TOE such as Microsoft Windows Server 2008.

12 For user verification to a web application server, user must use only compatible web browser such as Chrome 35, Mozilla Firefox 30 and Internet Explorer 11.

13 The data will be stored in Microsoft SQL Server 2012 where only System Admin is allowed to manage and maintain the database.

14 The end-user can communicate with the TOE through secure SSL channel provided by the TOE itself.

1.5 Clarification of Scope

15 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel, and secure communication in accordance with user guidance that is supplied with the product.

16 Section 1.4 of this document described the scope of the evaluation which was limited to those claimed made in the Security Target (Ref [6]). The TOE is a web application (Java-based) designed to be used as a Treasury Management Systems for a web-based application environment. The TOE operates depending on the medium storage, which contains the TOE files such as installer executable and supporting hardware required by the TOE to operate. Other components of Treasury Management System which includes the hardware appliance, operating system, medium storage specified in Section 1.5.3 of the Security Target (Ref [6]) are not part of TOE scope.

17 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

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

1.6.1 Usage assumptions

19 Assumption for the TOE usage as listed in Security Target :

a) The system admin who manages the TOE is not hostile and is competent.

b) The authorised user will keeps their passwords secret and not write them down or disclose them to any other system or user.

c) The authorised user will create a password which has a minimum of 8 and a maximum of 18 alphanumeric characters.

1.6.2 Environment assumptions

20 Assumptions for the TOE environment listed in Security Target are:

a) The TOE environment will provide appropriate authentication and authorisation controls for all users in the underlying environment (including database, network, operating system and application server).

b) The underlying operating system, application server and database are patched and hardened to protect against known vulnerabilities and security configuration issues.

c) The server hosting, the application and database servers are in a secure operating facility with restricted physical access and non-shared hardware.

d) The web application should has valid SSL certificates installed (not revoke or expired), and are sources from a trusted entity.

1.7 Evaluated Configuration

21 The TOE is a web application designed to be used as Treasury Management for a web-based application environment and shall be installed on dedicated host server running on compatible Windows Operating System as described in Section 1.6 of the Security Target (Ref [6]).

1.8 Delivery Procedures

22 d'COMPASS v2.0.0 is sent to the customers using delivery procedure (Ref **Error! Reference source not found.**), which ensures that the TOE is securely transferred from development environment to the responsibility of the customer. The brief delivery procedures are outlined below:

a) Ensuring that the underlying software/hardware platforms meet the required specifications; A schedule is given to customer via email or phone call regarding the delivery of the TOE to allow customer to know when the TOE is expected to be delivered by TriAset.

b) Software installation including the TOE and the underlying platform will be installed onsite by TriAset's representative along with the hardware specification.

c) Default account and passwords will be created by TriaAset's representative.

d) Upon completion of installation and configuration of the TOE, customer needs to complete the Application Installation Acceptance & Sign-off.

Note: Labelling, packaging and shipping of the TOE are not required as the TOE will be delivered and installed onsite by TriAset representative.

1.9 Documentation

23 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

24 The following documentation is provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

a) d'COMPASS Guidance Documentation v1.0, 1 October 2014

b) d'COMPASS Lifecycle Documentation v1.0, 1 October 2014

c) d'COMPASS Product Installation Guide v1.03, 29 September 2014

d) d'COMPASS SSL Setup Guide V1.01, 4 August 2014

2 Evaluation

25 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

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

2.1.1 Life-cycle support

27 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.

28 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

29 The evaluators analysed 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).

30 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 behaviour of the SFR-enforcing subsystems.

31 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.

2.1.3 Guidance documents

32 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.

2.1.4 IT Product Testing

33 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from CyberSecurity Malaysia MySEF (CSM MySEF). The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

34 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, 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).

35 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

36 At EAL2, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented developer tests.

37 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
Test Group A.1 and A.2 • to test on how system administrator configures the setting for configuration, security and password	• Access control • Identification and Authentication • Security Management	ADMIN Interface	**PASS.** Result as expected.

Test Group B.1, B.2 and B.3 • To test on how user accesses the protected resources with the privileges given and business configuration that can be managed by user.	• Access control • Identification and Identification • Security Management	• User Interface	**PASS.** Result as expected.
Test Group C • To test on how SSL is implemented at SSL_API in securing the communication for TOE access.	• Secure Communication	• SSL_API	**PASS.** Result as expected.

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

2.1.4.3 Penetration Testing

39 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.

40 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 (elapse 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 requirement for exploitation.

41 The penetration tests focused on:

a) Scanning for Secure Communication

b) Sniffing for Identification & Authentication and Secure Communication

c) Injection for Identification & Authentication

d) Cross Site Scripting (XSS) for Identification & Authentication

e) Broken Authentication and Session Management for Identification & Authentication, Secure Management and Access Control

f) Password Attack for Identification & Authentication

g) Directory Traversal for Access Control and Identification & Authentication

42 The results of the penetration testing note 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 1.5.3 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

43 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.

3 Result of the Evaluation

44 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 d'COMPASS v2.0.0 performed by CyberSecurity Malaysia MySEF.

45 CyberSecurity Malaysia MySEF, found that d'COMPASS v2.0.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentations, and has met the requirements of the Common Criteria (CC) assurance level 2 (EAL2).

46 Certification is not 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

47 EAL2 provides assurance by a full security target and analysis of the SFRs in that Security Target, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

48 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.

49 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

50 In addition to ensure secure usage of the product, below are additional recommendations for d’COMPASS v2.0.0 users:

a) Potential purchasers 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.

Annex A References

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] d'COMPASS Security Target, v1.0, 1 October 2014.

[7] E036 Evaluation Technical Report for d'COMPASS v2.0.0, v1.0, 3 December 2014.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
Authentication Data	It is information used to verify the claimed identity of a user.
ACL	Access control lists
Java EE	Java Platform Enterprise Edition
RDBMS	Relational database management system
SHA-256	SHA stands for Secure Hash Algorithm. SHA-256 is a set of cryptographic functions that fails under SHA-2 family designed by the U.S. National Security Agency (NSA) and published in 2001 by the NIST as a U.S. Federal Information Processing Standard (FIPS)
CCRA	Common Criteria Recognition Arrangement
System Admin	The system admin is a pre-set user within the TOE that is created during TOE installation. All functions assigned to System admin are add new user profile and roles, edit/change and delete existing user profile and role setting, cancelling the form changes, closing the form, change password, and security setting
EAL	Evaluation Assurance Level
TSF data	Data created by and for the TOE, which might affect the

Acronym	Expanded Term
	operation of the TOE.
TSC	TOE Scope of Control, the set of interactions that can occur with or within a TOE and are subject to the rules of the TSP
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.
Unauthorized users	Unauthorized users can mean a legitimate user with access rights to certain web resource, an external entity that has no rights to any protected resource or data.
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MySEF	Malaysian Security Evaluation Facility
Users	It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, there are users of the TOE access the TOE through a web browser.
User data	Protection Profile

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
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.
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.
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.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

--- END OF DOCUMENT ---