CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

C028 Certification Report

eWorkshop Version 1.0

File name: MyCB-5-RPT-C028-CR-v1a
Version: v1a
Date of document: 13 January 2011
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 8, Block A
Mines Waterfront Business Park
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8946 0999

C028 Certification Report
eWorkshop Version 1.0

13 January 2011
MyCB Department

CyberSecurity Malaysia
Level 8, Block A, Mines Waterfront Business Park,
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan, Selangor, Malaysia
Tel: +603 8946 0999 □ Fax: +603 8946 0888
http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C028 Certification Report - eWorkshop Version 1.0
DOCUMENT REFERENCE:	MyCB-5-RPT-C028-CR-v1a
ISSUE:	v1a
DATE:	13 January 2011

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright and Confidentiality Statement

Registered office:

Level 8, Block A,

Mines Waterfront Business Park,

No 3 JalanTasik, The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Forward

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) established within 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 13 January 2011, 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.

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 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (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
v1	22 December 2010	All	Released
v1a	31 January 2011	Page iv	Add the date of the certificate.

Executive Summary

The eWorkshop Version 1.0 (hereafter referred as eWorkshop Version 1.0) from Triangle Sphere Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

eWorkshop Version 1.0 is an intranet web based application for managing a vehicle maintenance workshop, suitable for an entity that has a fleet of vehicles to maintain or is contracted to maintain vehicles.

The TOE is software that comprises of:

- eWorkshop Version 1.0, a web based application that facilitates the registration, transaction recording, consolidation and reporting of vehicle particulars, cost and service particulars, and, part and stock particulars.

Part of eWorkshop Version 1.0 that is within the scope of evaluation is the Access Control Administration which covers the security function include creation and deletion of logon IDs for users, assignment of user roles, and security audit that logs records pertaining to creation, update, deletion of IDs.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for eWorkshop Version 1.0, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, 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 eWorkshop Version 1.0 to the Common Criteria (CC) evaluation assurance level EAL1. The report confirms that the product has met the target assurance level of EAL1 and the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the CyberSecurity Malaysia MySEF and completed on 2 December 2010.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the eWorkshop Version 1.0 evaluation meets all the conditions of the MyCC Scheme requirements and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

It is the responsibility of the user to ensure that the eWorkshop Version 1.0 meets their requirements. It is recommended that a potential user of the eWorkshop Version 1.0 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

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 eWorkshop version 1.0 is an intranet web based application for managing a vehicle maintenance workshop, suitable for an entity that has a fleet of vehicles to maintain or is contracted to maintain vehicles. The TOE is software that comprises of:

a) eWorkshop Version 1.0, a web based application that facilitates the registration, transaction recording, consolidation and reporting of vehicle particulars, cost and service particulars, part and stock particulars.

1.2 TOE Identification

2 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	C028
TOE Name	eWorkshop Version 1.0
TOE Version	Version 1.0
Security Target Title	eWorkshop Version 1.0 Security Target
Security Target Version	1-6
Security Target Date	19 November 2010
Assurance Level	Evaluation Assurance Level 1 (EAL1)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL1
Sponsor and Developer	Triangle Sphere Sdn Bhd Suite 8.09, Level 8, Wisma Zelan, No 1, Jalan Tasik Permaisuri 2, Bandar Tun Razak, 56000 Kuala Lumpur Malaysia

	Tel: 603 – 9173 6104 Fax: 603 – 9173 7105
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

3 eWorkshop Version 1.0 implements Administrator Policy, and User Policy:

a) The Administrator Policy is to allow the administrator to perform the dual function of logon ID and user role administration, as well as the correction of erroneous data or misaligned data entries entered by the other users.

b) The User Policy enables the user to access their authorised functions via the screens associated with the user role.

4 The details of the security policy are described in Section 6 of the Security Target (Ref [6]).

1.4 TOE Architecture

5 eWorkshop Version 1.0 includes both logical and physical boundaries.

1.4.1 Logical Boundaries

6 Figure 1 below describes the components of eWorkshop Version 1.0 that comprise the TOE;

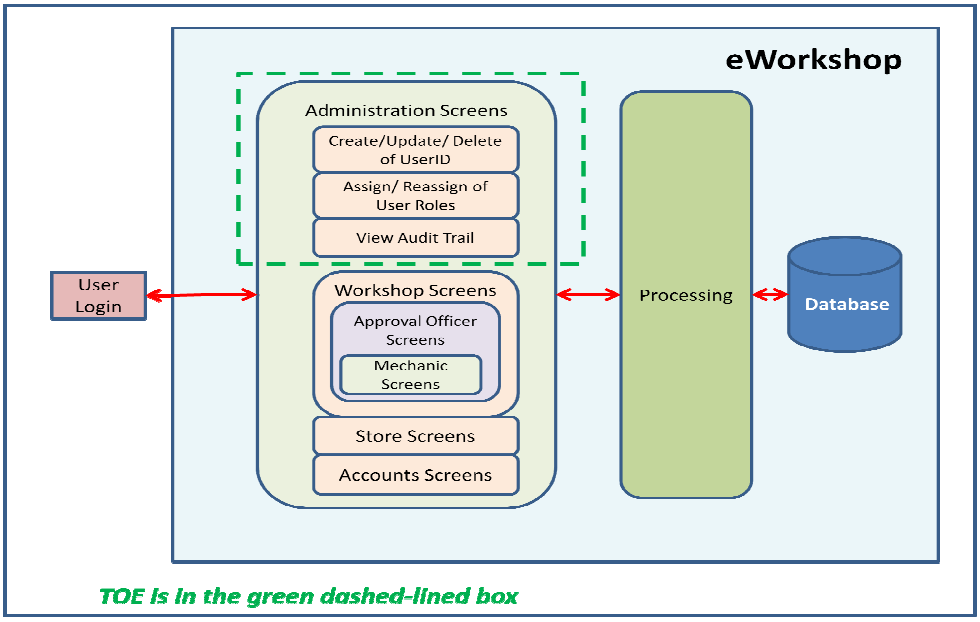

Figure 1: TOE Logical Scope

7 The TOE security functions comprises of the following:

a) Creation of Logon IDs for authorised users and deletion of Logon IDs for users who have left the organisation.

b) Assignment of user roles to authorised users so that the users can access the screens and functions to perform their designated responsibilities (and nothing else).

c) Security Audit that logs records pertaining to creation, update, delete of IDs, protection of data by authorising the access by role, Session locking after 15 minutes of idle, and time stamp from underlying OS to protect the TSF.

1.4.2 Physical Boundaries

8 Physically, the TOE is an application that requires a server with 2GHz or faster processor, operating system, web server, database and other supporting softwares as described in Section 1.3.3 of the Security Target (Ref [6]).

9 The Security Target assumes that the application server is to be located in a secure area that is free from physical access to unauthorised parties. This would restrict access to the application through only logical access.

1.5 Clarification of Scope

10 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) **Identification, Authentication and Authorization** - The assignment of usernames and passwords is done inside the Administrator module. The TOE requires authorized users and administrators to log in to the application system using their usernames and passwords before they can access data and relevant modules.

b) **Security Audit** - The auditing security function of the TOE is provided by the Administrator module. Record of Audit data is stored in the eWorkshop Version 1.0 database. All recorded audit data can only be viewed and deleted by authorized administrators. There are two (2) different types of audit data collected on two (2) different types of users.

i) Login Logs – successful and unsuccessful login activities of administrator and users

ii) Admin Activity Logs – activities by administrator on creation, update, delete of user IDs and resetting of passwords for users.

c) **Security Management** - The Administrator module allows authorized administrators to create user accounts and assign them unique usernames and passwords for accessing the TOE. Through the assignment of user roles by the authorized administrator, the user is authorised and restricted to perform the appropriate functions of creation, update and delete of information within the appropriate role boundary.

d) **TOE Access** - Inactive sessions are logged out after 15 minutes of user inactivity. The users are automatically logged out and returned to the login page. Pressing the back button on the internet browser causes the TOE to

automatically redirect them to the login page. The TOE assumes that the operational environment provides a reliable time stamp source.

e) **User Data Protection** - Access to the application functions is controlled by the user role assigned to the user. The user role must be assigned by the authorized administrator upon approval through procedures outside of the application.

f) **Protection of TSF** - To protect the integrity of the TOE, a reliable time stamp is required to be used in association with audit trail activities. The time stamp is provided by the operating system.

11 Potential consumers of the TOE are advised that some functions and services may not have been evaluated as part of the evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

12 Functions and services which are not included as part of the evaluated configuration are as follows:

a) A Hardware Server;

b) An Operating System on which the TOE is installed on;

c) A Database Software on which the TOE is dependent on as its database;

d) Microsoft Internet Information Services Web Server (included in the operating system);

e) Other supporting software;

i) Microsoft .NET Framework Version 2.0

ii) Web browser known as Microsoft Internet Explorer 7.

1.6 Assumptions

13 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the eWorkshop Version 1.0 as defined in subsequent sections and in the Security Target.

1.6.1 Usage assumptions

14 This evaluation was performed at EAL1. Therefore, no assumption for the TOE usage was provided for the TOE.

1.6.2 Environment assumptions

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

a) The TOE users must be authorized by the management before user ID and user role being assigned for them to access and use the TOE in a secure manner.

b) The TOE users received appropriate training before allowing them to work and use the TOE.

c) The TOE will be installed in a physically secured location and the use of the TOE will be confined to the intranet environment without access to the internet.

1.7 Evaluated Configuration

16 The TOE is to be configured according to the Preparative User Guidance (Ref22a)).

17 The TOE is delivered to the customer by the developer's trusted personnel. The developer's personnel then install the TOE and make changes to configuration based on Preparative User Guidance (Ref 22a)) as following:

a) Database server installation and configuration.

b) Internet Information Service Activation.

c) Dotnetfx installation.

d) eWorkshop Version 1.0 application installation and configuration.

1.8 Delivery Procedures

18 eWorkshop Version 1.0 is delivered to the user by the developer's authorised personnel.

19 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, developer did not provide any documentation on TOE delivery and the evaluators did not verify any TOE delivery process.

1.9 Documentation

20 To ensure continued secure usage of the product, it is important that the eWorkshop Version 1.0 is used in accordance with guidance documentation.

21 The following documentation is provided by the developer to the end user as guidance to ensure secure operation of the product:

a) eWorkshop User Manual, version 1.0, 29 October 2010.

b) eWorkshop Administrator Manual, version 1.0, 29 October 2010.

22 The following documentation is used by the developer's authorised personnel as guidance to ensure secure installation of the product:

a) eWorkshop Preparatory Procedures, version 1.0, 11 November 2010.

2 Evaluation

23 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). 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

24 The evaluation activities involved a structured evaluation of eWorkshop Version 1.0, including the following components:

2.1.1 Life-cycle support

25 An analysis of the eWorkshop Version 1.0 configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled.

2.1.2 Development

26 The evaluators analysed the eWorkshop Version 1.0 functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

2.1.3 Guidance documents

27 The evaluators examined the eWorkshop Version 1.0 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

28 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The eWorkshop Version 1.0 testing was conducted at CyberSecurity Malaysia MySEF where it was subjected to an independent functional and penetration tests. 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 Independent Functional Testing

29 At EAL1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining functional and guidance documentation, and creating test cases to verify the behaviour of the TOE.

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

Table 2: Independent Functional Testing

TEST TITLE	DESCRIPTION	SECURITY FUNCTION	TSFI
TEST GROUP A	**Test Group A** comprises a series of test cases on TOE security functions of web based for **audit records generation and time stamp** for relevant authentication and management events.	Security Audit	User and Administrator Login Audit Trail
TEST GROUP B	**Test Group B** comprises a series of test cases on TOE security functions of how **TOE control access and privilege** for each user.	User Data Protection	Administrator Page Employee Profile Workshop Profile
TEST GROUP C	**Test Group C** comprises a series of test cases on TOE security functions of **identification and authentication** of administrator and user through web portal.	Identification and Authentication	User and Administrator Login Change Password Automated Random Password Generation
TEST GROUP D	**Test Group D** comprises a series of test cases on TOE security functions of **management function** for administrator in web portal	Security Management	User and Administrator Login Create/Update/ Delete Employee Create/Update/ Delete Profile Automated Random Password Generation
TEST GROUP E	**Test Group E** comprises a series of test cases on TOE security functions of **monitoring user session** in web portal.	TOE Access	Session Timeout

31 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.2 Penetration Testing

32 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, and functional specification.

33 From the vulnerability analysis, the evaluators conducted penetration testing to determine whether potential vulnerabilities could be exploited in the intended operating environment of the TOE, 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;

d) Window of opportunity; and

e) IT hardware/software or other requirement required for exploitation.

34 The penetration tests focused on:

a) Generic vulnerabilities;

b) Bypassing;

c) Tampering; and

d) Direct attacks.

35 The results of the penetration testing note that a number of additional vulnerabilities exist that are dependent on an attacker effort, time, skill/knowledge, and focused tools/exploits use to gather the TOE configuration information. Therefore, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.3 Testing Results

36 Tests conducted for the eWorkshop Version 1.0 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

3 Result of the Evaluation

37 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 eWorkshop Version 1.0 performed by the CyberSecurity Malaysia MySEF.

38 The CyberSecurity Malaysia MySEF found that eWorkshop Version 1.0 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL1.

39 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. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

40 EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a functional and interface specification and guidance documentation, to understand the security behaviour.

41 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functions.

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

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

3.2 Recommendation

44 In addition to ensure secure usage of the product, below are additional recommendations for eWorkshop Version 1.0 consumers:

a) HTTPS is recommended to be deployed in TOE environment by the server to ensure that the communication between client and server is encrypted.

b) Use the product only in its evaluated configuration.

c) Ensure strict adherence to the delivery procedures.

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 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

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

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

[6] eWorkshop Version 1.0 Security Target, Version 1-6, 19 November 2010

[7] Evaluation Technical Report eWorkshop Version 1.0, Version 1.2, 2 December 2010

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 Standards Organisation
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.
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.
MyCB Personnel	Includes all members of the Certification Subcommittee, the Scheme Manager, the Senior Certifier, Certifiers and the Quality Manager.

Term	Definition and Source
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 ---