CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

# C018 Certification Report
# IDOTTV Web Portal version 2.0

File name: ISCB-5-RPT-C018-CR-v1
Version: v1
Date of document: 8 February 2011
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme™
MyCC

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

# C018 Certification Report
# **IDOTTV Web Portal version 2.0**

8 February 2011

ISCB 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:*** | C018 Certification Report - IDOTTV Web Portal version 2.0 |
| ***DOCUMENT REFERENCE:*** | ISCB-5-RPT-C018-CR-v1 |
| ***ISSUE:*** | v1 |
| ***DATE:*** | 8 February 2011 |

| | |
|---|---|
| ***DISTRIBUTION:*** | UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION |

# Copyright 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) 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 8 February 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.

Reproduction of this report is authorized 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 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 | 8 February 2011 | All | Final Released. |

# Executive Summary

IDOTTV Web Portal 2.0 (hereafter referred as IDOTTV Web Portal 2.0) from IDOTTV Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The IDOTTV Web Portal 2.0 is an online web application system that enables users (of the system) to see the polling result, and read SMS and MMS sent by public after reading the organization’s published magazines. The scope of the evaluation covers Administrator’s module and Administrator and user login page.

The IDOTTV Web Portal 2.0’s administrator modules comprise of components such as login, user, audit trail, change password, logout, message summary, message approved, message exported, question, polling, report publication, and report originator.

Those components like login, user, audit trail, change password, logout are included in the scope of evaluation. The message summary, message approved, message exported, question, polling, report publication, and report originator are out of scope of the evaluation.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for IDOTTV Web Portal 2.0, the security 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 IDOTTV Web Portal 2.0, to the Common Criteria (CC) evaluation assurance level EAL2. The report confirms that the product has met the target assurance level of EAL2 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 was completed on 17 January 2011.

# Table of Contents

# Index of Tables

# Index of Figures

# 1 Target of Evaluation

## 1.1 TOE Description

1 The Target of Evaluation (TOE), IDOTTV Web Portal version 2.0, is an online web application system that enables users (of the system) to see the polling result, and read SMS and MMS sent by public after reading the organization's published magazine. This online application supports for identification and authentication of the user and administrator, security audit in generating audit logs, user data protection in controlling account privilege for the user, TOE Access, and security management of the TOE.

2 The TOE is installed on a web server in providing the particular function for publications. The hardware and software where the TOE is installed is not included in the evaluation scope. The TOE and its guidance documentations are delivered to the clients in CDs by the authorized person from IDOTTV Sdn Bhd.

3 Note that administrators are those who handle administrative tasks of IDOTTV Web Portal version 2.0 like creating, editing, and deleting users; setting user privileges; and, view audit trails. Users are those who operate the IDOTTV Web Portal version 2.0. For example, a user can be an editor who can publish tips or news.

## 1.2 TOE Identification

4 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** | C018 |
| **TOE Name** | IDOTTV Web Portal 2.0 |
| **TOE Version** | 2.0 |
| **Security Target Title** | IDOTTV Web Portal 2.0 Security Target |
| **Security Target Version** | 1.11 |
| **Security Target Date** | 17 January 2011 |
| **Assurance Level** | EAL 2 |
| **Criteria** | CC Part 1, CC Part 2, CC Part 3 Revision 3 (Ref [2]) |
| **Methodology** | Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]) |
| **Protection Profile Conformance** | None. |
| **Common Criteria Conformance** | CC Part 2 Extended. |

| | |
|---|---|
| | CC Part 3 Conformant.<br>Package conformant to EAL2. |
| **Sponsor and Developer** | IDOTTV Sdn Bhd,<br>Level 10, Kelana Parkview Tower,<br>Jalan ss6/2,<br>47301 Petaling Jaya,<br>Phone: +60378802001<br>Fax: +60378806001 |
| **Evaluation Facility** | CyberSecurity Malaysia MySEF |

## 1.3 Security Policy

5 IDOTTV Web Portal 2.0 implements access control policy to restrict access to the TOE. The administrator is responsible to assign user's access based on the user's role. The user needs to provide correct username and password in order to access the TOE.

## 1.4 TOE Architecture

6 IDOTTV Web Portal 2.0 includes both logical and physical boundaries which are described in Section 2.3 of the Security Target (Ref [6]).

7 Figure 1 and Figure 2 below describes the components of IDOTTV Web Portal 2.0 that comprise the TOE:

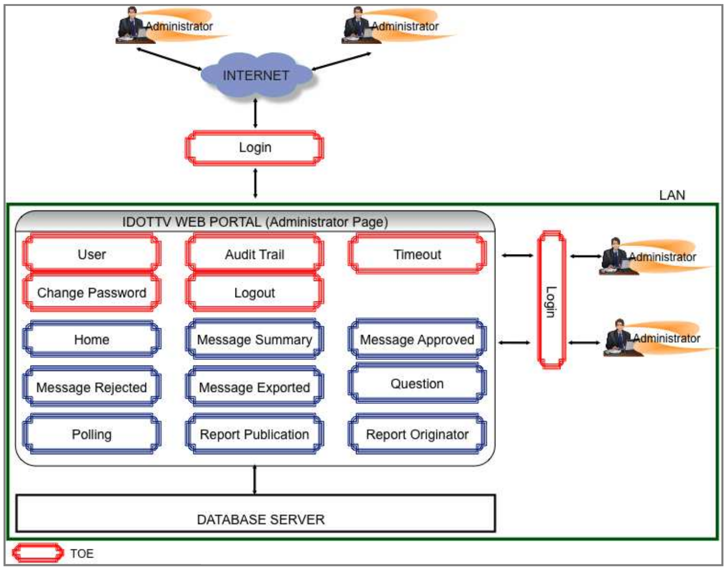

Figure 1: Modules under Administrator page

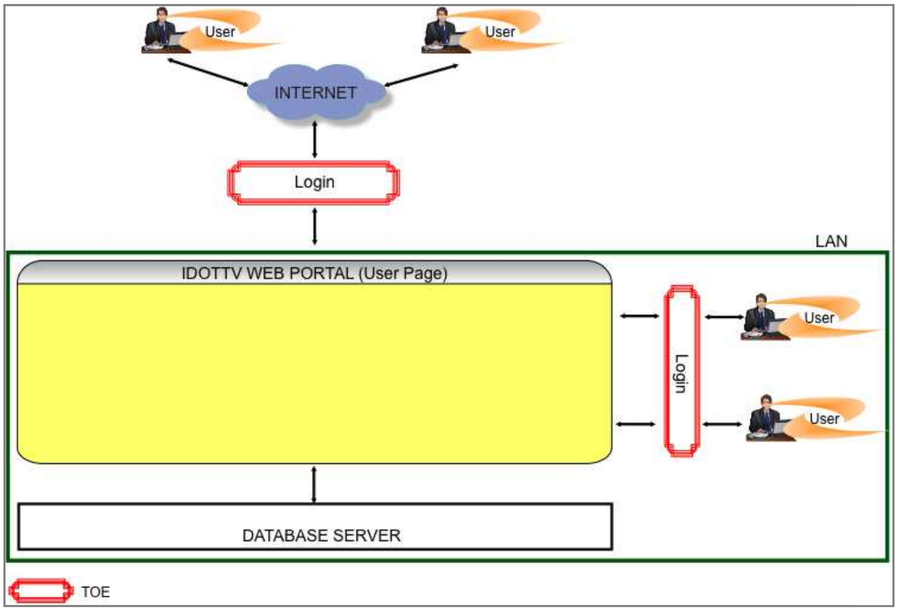

Figure 2: Login module for User

8 Following are the security architectural descriptions of each component of the TOE:

a) **Login**: This component allows the administrators and users to log into the Web Portal. Once logged in, the administrators will be directed to the Administrator Page to perform administrator functions. for the user, once they are logged in, they will be directed to their user pages (note that the user pages and the resources/functions that the users have access to are not part of the scope of the TOE).

b) **User**: This component allows the administrators to add, edit and delete user/administrator accounts. It also allows administrators to reset/unlock passwords for those accounts.

c) **Audit trail**: Authorized administrators are allowed to view the audit logs for all user/administrator accounts. They however, cannot edit or delete the logs captured. This will allow the administrator to analyze the logs for possible unauthorized attempts to the resources.

d) **Timeout**: This component allows the administrators to specify the timeout session. Inactive sessions are logged out after this defined period of inactivity and the administrator/users are automatically returned to the login page. The default value is 15 minutes.

e) **Change password**: Administrators can change their passwords by clicking on the Change Password button.

f) **Logout**: To allow authorized administrators to logout of the Web Portal.

9 The separate security domains architected into the TOE are as follows:

a) **Separate service/server**: As seen in the figures above, the web portal service and database service are separated logically (or physically) to ensure that users and administrators do not access the database service directly. All access to the database must be done via the web portal.

b) **Administrator domain**: The TOE is designed where only authorized administrators can access the administrator page on the web portal.

## 1.5 Clarification of Scope

10 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 communication security in accordance with administrator guidance that is supplied with the product. 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) **Security Audit** - The TOE generates audit logs that consist of various auditable events or actions as listed in Table 13 of the Security Target (Ref [6]). Date and time of events, usernames, and events taken by the authorized users are recorded.

b) **User Data Protection** - Authorized administrators of the TOE can perform the following functions to the user or administrator accounts:

i) Account creation for users and additional administrators that includes the assignment of usernames and passwords.

ii) Access privilege assignments by user levels.

iii) Reset and unlock passwords for authorized users.

iv) Change password for own administrator.

c) **Identification and Authentication** - provides the TOE with the ability to govern access by users and administrators. An administrator can manage the

TOE through the IDOTTV Web Portal version 2.0, a web-based graphical user interface.

d) **Security Management** - The authorized administrators are able to create user accounts and assign them usernames and first time passwords for accessing the TOE. An administrator also has the ability to create other administrator accounts. At least one administrator is required to have full access rights to manage the TOE.

e) **TOE Access** - Authorized administrators can define the session expiration time (in minutes). After inactivity of the specified period, the authorized users are then returned to the main page of the IDOTTV web portal. The TOE assumes that the operational environment of the IDOTTV web portal provides a reliable time stamp source.

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 Figure 1 and Figure 2 in Section 1.4 of this document show the scope of the evaluation.

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

a) A Hardware Server (Xeon Quad Core, processor speed of 2.00 Ghz, RAM of 4GB);

b) An Operating System (Windows Server 2003);

c) Database (MySQL version 5.0.77);

d) Firewall;

e) Other supporting software;

   i) Web Browser (Mozilla Firefox 3.6.13, Internet Explorer 8).

   ii) PHP Interpreter (PHP version 5.1.6).

   iii) Apache Web Server version 2.2.3.

## 1.6 Assumptions

14 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 IDOTTV Web Portal 2.0 as defined in subsequent sections and in the Security Target.

### 1.6.1 Usage assumptions

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

a) The third party applications that the TOE relies upon have been configured in accordance with the installation guides. They are securely configured in such a way that the applications provide protection for the TOE from any unauthorized users or processes.

b) There are one or more competent individuals that are assigned to manage the TOE and its secured data. Such personnel are assumed not to be careless, wilfully negligent or hostile.

### 1.6.2 Environment assumptions

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

a) All hardware within the environment, including network and peripheral devices, has been approved for the transmitting of secured data. Each of these appliance configurations is securely managed by administrators to provide protection of secured data in terms of its confidentiality and integrity.

## 1.7 Evaluated Configuration

17 This section describes the configurations of the TOE that are included within the scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the Preparative User Guidance (Ref 25a)).

18 The TOE is delivered in a CD, as an application, by the developer's authorised personnel. The developer's authorised personnel is responsible to make changes to the configuration based on Preparative User Guidance (Ref 25a)) as following:

a) IDOTTV Web Portal version 2.0 Installation

b) Configuring HTTPs on Linux

c) Import MySQL dump file using command

d) Import MySQL dump file using PhpMyAdmin

## 1.8 Delivery Procedures

19 IDOTTV Web Portal 2.0 is delivered to the user by the developer's authorised personnel to the user premises as described in Section 3 of the Preparative User Guidance (Ref 25a)). The process of the IDOTTV Web Portal version 2.0 delivery is outlined below.

20 The process begins when the client makes an order to purchase the IDOTTV Web Portal version 2.0 from IDOTTV. Once the client has agreed to purchase IDOTTV Web Portal version 2.0 via an issuance of Purchase Order, signing of a Contract or an issuance of a Letter of Award, the CD will be prepared.

21 The first CD contains the manuals for the clients, and the second CD is for the trusted IDOTTV staff to use for installation of the TOE.

22 The acceptance of the TOE is performed after a successful installation and testing by the client.

## 1.9 Documentation

23 To ensure continued secure usage of the product, it is important that the IDOTTV Web Portal 2.0 is used in accordance with guidance documentation.

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

a) IDOTTV Web Portal 2.0 Operative Guidance version 1.2, 13 December 2010.

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

a) IDOTTV Web Portal 2.0 Preparative Guidance version 1.5, 17 January 2011.

# 2 Evaluation

26 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 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

27 The evaluation activities involved a structured evaluation of IDOTTV Web Portal 2.0, including the following components:

### 2.1.1 Life-cycle support

28 An analysis of the IDOTTV Web Portal 2.0 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.

29 The evaluators examined Section 3 of the Preparative User Guidance (Ref 25a)) 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.

### 2.1.2 Development

30 The evaluators analysed the IDOTTV Web Portal 2.0 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).

31 The evaluators examined the IDOTTV Web Portal 2.0 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.

32 The evaluators examined the IDOTTV Web Portal 2.0 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

33 The evaluators examined the IDOTTV Web Portal 2.0 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

34 Testing at EAL2 consists of assessing developer tests, independent function test, and performing penetration tests. IDOTTV Web Portal 2.0 testing was conducted by tester from CyberSecurity Malaysia MySEF at CyberSecurity Malaysia MySEF Lab, CyberSecurity Malaysia, Seri Kembangan Selangor 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 Assessment of Developer Tests

35 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).

36 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

37 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 a sample of the developer's test plan, and creating test cases that augmented the developer tests.

38 The results of the independent test developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: List of Evaluator Independent Test

| Description | Security Function | TSFI | Results |
|---|---|---|---|
| To test whether admin can delete the audit logs and view if the audit logs provided the time stamp that generate by operational environment | Security Audit | TSFI Audit Trail | **PASS.** Result as expected**.** |
| To test whether the available fields on the TOE prevent from malicious code such as SQL Injection and XSS script | User Data Protection | TSFI User Data Protection | **PASS.** Result as expected**.** |
| To test the login process of the TOE provided the | Identification and | TSFI Authorized | **PASS.** Result as expected**.** |

| | | | |
|---|---|---|---|
| identification and authentication to govern access by users and administrators. | Authentication | User Login | |
| To test on function for administrator to manage user account where they are able to create user accounts and assign them default password and also delete own account. | Security Management | TSFI User Management | **PASS.** Result as expected**.** |
| To test a function for administrator to define session expiration time. | TOE Access | TSFI Timeout | **PASS.** Result as expected**.** |

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

#### 2.1.4.3 Penetration Testing

40 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.

41 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist 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.

42 The penetration tests focused on :

a) Generic vulnerabilities;

b) Web based penetration testing;

c) Tampering.

43 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.

#### 2.1.4.4 Testing Results

44 Tests conducted for the IDOTTV Web Portal 2.0 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

# 3 Result of the Evaluation

45 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 IDOTTV Web Portal 2.0 performed by the CyberSecurity Malaysia MySEF.

46 The CyberSecurity Malaysia MySEF found that IDOTTV Web Portal 2.0 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 EAL2.

47 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

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

49 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.

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

## 3.2 Recommendation

51 In addition to ensure secure usage of the product, below are additional recommendations for IDOTTV Web Portal 2.0 consumers:

a) Encrypt user credential such as username and password with a strong hashing/encryption algorithm.

b) Configuration of the environment such as web server, database and operating system running the IDOTTV Web Portal 2.0 should also be hardened to prevent any vulnerability from being disclosed.

c) Use the IDOTTV Web Portal 2.0 only in its evaluated configuration.

d) 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] IDOTTV Web Portal 2.0 Security Target, Version 1.11, 17 January 2011.

[7] Evaluation Technical Report IDOTTV Web Portal 2.0, Version 1.2, 17 January 2011.

## 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 |
| 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. |
| 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. |

| Term | Definition and Source |
|---|---|
| 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 ---