C033 Certification Report

Mobile Billing System version 1.4

File name: ISCB-5-RPT-C033-CR-v1a
Version: v1a

Date of document: 15 June 2011

Document classification: PUBLIC

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

C033 Certification Report
Mobile Billing System version 1.4

15 June 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:	C033 Certification Report – Mobile Billing System version 1.4
DOCUMENT REFERENCE:	ISCB-5-RPT-C033-CR-v1a
ISSUE:	v1a
DATE:	15 June 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

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 15 June 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	2 June 2011	All	Final released.
v1a	15 June 2011	Page iv	Add the date of the certificate.

Executive Summary

IDOTTV Mobile Billing System Version 1.4 (hereafter referred as Mobile Billing System) from IDOTTV Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

The Mobile Billing System is software that facilitates secure, confidential, and paperless billing services between service provider and the customers which is installed on a user's mobile device. It comprises of three components:

- **Mobile Billing Applet.** A java-based mobile application developed specifically for the Blackberry mobility platform. The application provides a subscriber with the basis for integrating with the mobile billing server.
- **Mobile Billing Server**. An application that provides connectivity to the billing systems of telecommunication providers, and the mobile billing applet application for subscribers. It also provides storing data for the TOE.
- **Mobile Billing Webtool.** A web-based interface for both subscribers and administrators to login and manage their accounts or the system.

The part of the Mobile Billing System that covered under scope of evaluation is identification and authentication (user login), secure communication between Mobile Billing server with the Mobile Application, user data protection which is user access based on the user level, and security management of the TOE which focusing on account management activities such as create user account, reset the password and change the access level for telecommunication company.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for Mobile Billing System, 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 Mobile Billing System, 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 stratsec Security Evaluation Facility (STRATSEF) and was completed on 30 May 2011.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the Mobile Billing System evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

It is the responsibility of the user to ensure that the Mobile Billing System meets their requirement and security needs. It is recommended that prospective users of the Mobile Billing System refer to the ST (Ref [6]), and read this Certification Report prior to deciding whether to purchase and deploy the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The TOE is IDOTTV Mobile Billing System version 1.4 (hereafter referred as Mobile Billing System) that provides a central point for managing customer billing information for telecommunications providers, in order to facilitate secured, confidential and paperless billing. This system provides interfaces to the telecommunications provider's billing system, administrator, and to the users where the mobile application installed on a user's device. It also features a mobile payment function that enables customers to make bill payment via mobile device.

2 The TOE is comprised of three key components:

a) **Mobile Billing Applet** - A java-based mobile application developed specifically for the Blackberry mobility platform. The application provides a subscriber with the basis for integrating with the mobile billing server.

b) **Mobile Billing Server**- An application that provides:

i- Connectivity to the mobile billing systems of telecommunications providers.

ii- A connection to the mobile billing applet that provides subscribers with system connectivity.

iii- Storing data for the TOE

c) **Mobile Billing Webtool** - A web-based interface for both subscriber and administrators to login and manage their accounts or the system.

3 The evaluated security functionalities for the TOE includes:

a) **Identification and Authentication** - provides identification and authentication of the TOE users.

b) **User data protection** - The TOE will permit a user to access the billing information only if a userID or role of the user has permission to perform the requested action on the information.

c) **Security Management** - managing user management functions through the use of the Web Administration Interface as well as through the applet installed on mobile devices to ensure that the functions are restricted to only those users that need to have access to privileged functions.

d) **Secure Communication** - protection of the billing information from disclosure and modification when the scanned data is sent from Mobile Billing server to the applet application.

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	C033
TOE Name	Mobile Billing System (consist of Mobile Billing Webtool version 1.4, Mobile Billing Applet version 1.0 and Mobile Billing Server version 1.0)
TOE Version	1.4
Security Target Title	IDOTTV Mobile Billing System Security Target
Security Target Version	1.2
Security Target Date	25 May 2011
Assurance Level	EAL 1
Criteria	Common Criteria Part 1, Common Criteria Part 2, Common Criteria Part 3 Revision 3 (Ref [2])
Methodology	Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3])
Protection Profile Conformance	No conformance to any PP.
Common Criteria Conformance	- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1, Revision 3, July 2009 - Part 3 conformant, Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 3, July 2009. - Package conformant to EAL1.
Sponsor and Developer	IDOTTV Sdn Bhd, Level 10. Kelana Jaya Parkview Tower, Jalan SS6/2, 47301 Petaling Jaya, Phone: +60378802001 Fax: +60378806001
Evaluation Facility	stratsec.net SDN BHD known as STRATSEF

1.3 Security Policy

5 Mobile Billing System does implement Access Control Security Function Policy (SFP) to restrict the access level of the user based on their role stored in the Access Control Lists. The roles maintained by the TOE are:

a) Telecommunication Administrator – can see all the billing information.

b) Mobile Subscriber – can only see their billing information.

c) Super Administrator – can see all the billing information.

d) Telecommunication Employee – will be up to the Telecommunication Administrator or Super Administrator to configure the access.

6 The details of the access control security function policy are described in Section 4.3 of the Security Target (Ref [6]).

1.4 TOE Architecture

7 Mobile Billing System includes both logical and physical boundaries.

1.4.1 Logical Boundaries

8 The logical boundary consists of the security functionality of TOE is summarized below:

a) **Identification and Authentication** – The TOE requires the user to identify and authenticate themselves before accessing any information and performing any actions. The TOE will check the credentials presented by the user upon the login page against the authentication information in the database.

b) **Security Management** – The TOE provides various user management functions to ensure efficient and secure management of the TOE.

c) **User Data Protection** – The TOE provides its own access control between subjects and objects covered by the User Access Control Security Function Policy.

d) **Secure Communication** – The TOE is able to protect the billing information from disclosure and modification when the scanned data is sent from Mobile Billing Server to the applet application.

1.4.2 Physical Boundaries

9 Physically, the TOE is an application that consists of the applet installed on Java enabled mobile devices as well as Mobile Billing Server which runs Apache HTTP Server version 2.0 on a Linux Operating System (CentOS 5) as described in Section 1.4.1 of the Security Target (Ref [6]).

10 Administrator can access the TOE through a Web Admin interface using Mobile Billing Webtool version 1.4 and user will access the TOE via application installed on their Blackberry phone using Mobile Billing Applet version 1.0.

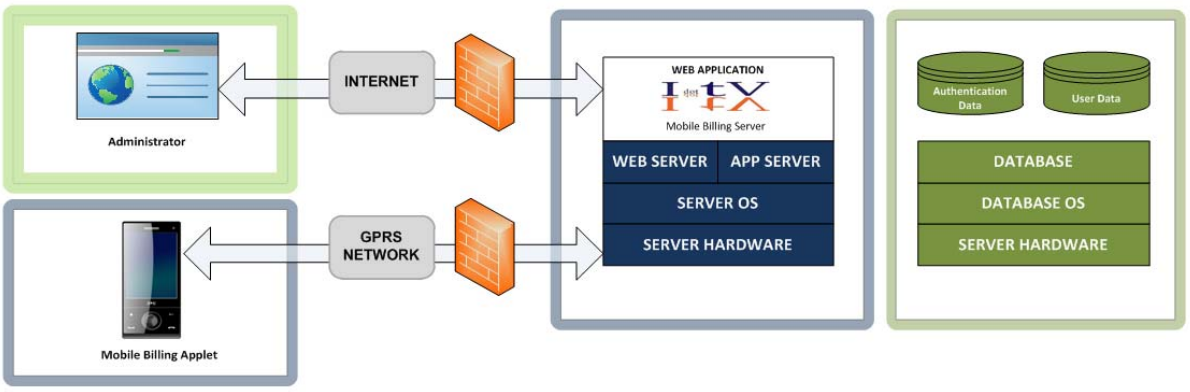

Figure 1: The components of Mobile Billing System

1.5 Clarification of Scope

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

a) **Identification & Authentication** – When a user issues a request to the TOE to access the user's billing information, the TOE requires that the user identify and authenticate themselves before performing any actions on behalf of the user. The TOE checks the credentials presented by the user upon the login page against the authentication information in the database. Mobile Subscriber will login through the interface provided by the Mobile Billing applet on their mobile device. For the Telecommunication Administrator, Telecommunication Employee and the Super Administrator, they will login through the Mobile Billing Webtool (web portal).

Mobile Billing Server is responsible to hash users' password before being used to authenticate the user or when users change their passwords, and is being written to the database.

b) **User Data Protection** – The TOE maintained four types of user: Mobile Subscriber, Telecommunication Administrator, Telecommunication Employee and the Super Administrator. Each type of user will have different access rights to billing information. For mobile subscriber, they can only access their own billing information whereas administrator can access all information. All users will have a unique user ID. The access control function permits a user to access the billing information, via Mobile Billing Applet, only if a userID or role of the user has permission to access the information.

Each Access Control List (ACL) maps users and roles to the operations that they are permitted to perform on the object. For the mobile subscriber, their userID, IMEI (International Mobile Equipment Identity is a unique 17 or 15 digit code used to identify an individual mobile station to a GSM or UMTS network), IMSI (International Mobile Subscriber Identity is a unique 15-digit code used to identify an individual user on a GSM network and a TAC code which is issued to the user during registration will be used to identify the user when they are accessing the billing information. This is to ensure that

only the user with the registered SIM card and phone can access the information.

c) **Security Management** – The TOE provides various management functions to ensure efficient and secure management of the TOE based on the type of TOE users as follows:

i- Mobile Subscriber

- Checking their account statement only.

ii- Administrator (Telecommunication)

- Authenticate to the Mobile Billing Server and as well as performing management functions according to their roles through the Mobile Billing Webtool.
- Only administrator and super administrators can change passwords, reset passwords and change the access levels of the telecommunication employees.
- Reset Password for user that forgot its password.

iii- Super Administrator

- Authenticate to the Mobile Billing Server and as well as performing management functions according to their roles through the Mobile Billing Webtool.
- Only administrator and super administrators can change passwords, reset passwords and change the access levels of the telecommunication employees.
- Create administrator users for the telecommunication company.

iv- Telecommunication Employees

- Authenticate to the Mobile Billing Server and as well as performing management functions according to their level that is allocated to them by the administrators or super administrator through the Mobile Billing Webtool.

The TOE allows no one to change the default values of the TOE security function (TSF) data and security attributes of the TOE as well as the access control list (ACL).

d) **Secure Communication** – The TOE provides a secure communication channel between the applet application and the Mobile Billing server when the billing information is transferred to and from the server. The initiation of the secure SSL channel is done by the Mobile Billing Applet on the Mobile Subscriber's mobile device. Whenever user launches the applet and proceeds to authenticate themselves, the Mobile Billing Applet will do a handshake protocol with the Mobile Billing Server and after this, a session key will be generated and will be used to encrypt the user data sent/retrieved to and from the Mobile Billing Server.

12 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.

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

a) Apache HTTP Server version 2.0;

b) An Operating System (Linux CentOS 5);

c) A Database Management System Software;

d) Other supporting gadgets;

i. Web Browser (Mozilla Firefox and Internet Explorer)

ii. BlackBerry phone; regardless the phone model.

1.6 Assumptions

14 This evaluation was performed at EAL1. Therefore, no assumptions for the TOE were defined in the ST (Ref [6]).

1.7 Evaluated Configuration

15 In principal, the TOE is to be configured according to the secure installation guidance (Ref 21).

16 The TOE is configured based on secure installation guidance (Ref 21) as following:

a) MySQL Installation.

b) SSL Setup.

c) Server Setup.

d) Subscriber Subscription and Installation.

e) Subscriber Application Guide.

1.8 Delivery Procedures

17 Subscriber for the Mobile Billing System will need to download and install the Mobile Billing Applet for their Blackberry mobile devices. They will be provided a link to download the applet once they subscribed with any respected Telco.

18 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

19 To ensure continued secure usage of the product, it is important that the Mobile Billing System is used in accordance with the guidance documentation.

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

a) MobileBilling Subscriber Application Guide (Ref [12]).

b) MobileBilling Web Portal User Guide (Ref [13]).

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

a) MobileBilling MYSQL Installation Guide (Ref [9]).

b) MobileBilling Server Setup Guide (Ref [14]).

c) MobileBilling Subscriber Subscription and Installation Guide (Ref [10]).

d) MobileBilling SSL Setup (Linux) Guide (Ref [15]).

e) MobileBilling Subscriber Application Guide (Ref [12]).

2 Evaluation

22 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

23 The evaluation activities involved a structured evaluation of Mobile Billing System, including the following components:

2.1.1 Life-cycle support

24 An analysis of the Mobile Billing System 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

25 The evaluators analysed the Mobile Billing System 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

26 The evaluators examined the Mobile Billing System 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

27 Testing at EAL1 consists of performing independent function test, and performing penetration tests. Mobile Billing System testing was conducted by tester from stratsec at IDOTTV Office, MTDC UPM, 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 Independent Functional Testing

28 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.

29 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 tests developed and performed by the evaluators to verify the TOE functionality are as follows:

Table 2: Independent Functional Testing

Description	Security Function	TSFI	Results
To test that the password of the user is protected using the MD5 algorithm method and is stored in the user database.	Identification and Authentication	• Authentication • Database Interface	Passed.
To test that normal user and administrator have specific security attribute in accessing the billing information and also controlling the data in the system	User data protection	• Web Portal Interface • User Information Database Interface	Passed.
To test that the access controls policy is implemented correctly within the TOE.	User data protection	• Web Portal Interface • User Information Database	Passed.
To test that user have to login before they can perform any action on that account	Identification and Authentication	• Mobile Device Interface • Authentication Database Interface	Passed.
To test that the TOE able to identified the login user as registered in database	Identification and Authentication	• Mobile Device Interface • Authentication Database Interface	Passed.
To test that only administrator have the control over write and delete security function.	Security Management	• Web Portal Interface • User Information	Passed.

		Database	
To test that there is restrictive default values for security attribute during the initialization process and TOE shall allow specifying alternative initial values to override the default values when an object or information is created.	Security Management	• Mobile Device Interface • User Information Database	Passed.
Run test to ensure that only the owner of password is able to modify or change	Identification and Authentication	• Web Portal Interface • User Information Database	Passed.
To test the TOE capabilities to perform the required management functions.	Security Management	• Web Portal Interface • User Information Database	Passed.
To test that the roles of normal user and administrator is maintained in the TOE and able to associate users with roles	User data protection	• Web Portal Interface	Passed.
To test that the data connection from mobile to server is secured and reliable.	Secure Communication	• Mobile Device Interface • Web Portal Interface	Passed.

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

2.1.4.2 Penetration Testing

31 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.

32 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.

33 The penetration tests focused on:

a) Web Based Exploit and Penetration Testing.

b) Mobile Penetration Testing.

34 The results of the penetration testing note that there is no exploitable and/or residual vulnerability found. However, 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

35 Tests conducted for the Mobile Billing System produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

36 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

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 Mobile Billing System performed by the STRATSEC Security Evaluation Facility (SEF) which known as STRATSEF.

38 The STRATSEF found that Mobile Billing System 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.

3.2 Recommendation

43 In addition to ensure secure usage of the product, below are additional recommendations for Mobile Billing System consumers:

a) Password strength, such as length and level of complexity for the user and administrator accounts should be enforced.

b) The user must ensure that they will only use the TOE in secure manner according to the secure operational user guidance.

c) Use it only in its evaluated configuration.

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 Mobile Billing System Security Target, Version 1.2, 25 May 2011.

[7] Evaluation Technical Report EAL1 Evaluation of IDOTTV, Version 1.2, 30 May 2011.

[8] Mobile Billing System Evaluation Guidance Documentation, Version 0.4, 25 May 2011.

[9] MobileBilling MYSQL Installation Guide version 1.0, 20 September 2010.

[10] MobileBilling Subscriber Subscription and Installation Guide version 1.0, 20 September 2010.

[11] MobileBilling Web Portal User Guide version 1.0, 20 September 2010.

[12] MobileBilling Subscriber Application Guide version 1.0, 20 September 2010

[13] MobileBilling Web Portal User Guide version 1.0, 5 October 2010.

[14] MobileBilling Server Setup Guide version 1.0, 2 November 2010.

[15] MobileBilling SSL Setup (Linux) Guide version 1.0, 2 November 2010.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
ALC	Access Control List
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement

Acronym	Expanded Term
IEC	International Electrotechnical Commission
ISO	International Organization of Standardization
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
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TOE Security Functionality Interface

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.
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 ---