CyberSecurity MALAYSIA
An agency under MOSTI

People First, Performance Now

MOSTI
Ministry of Science, Technology and Innovation

C038 Certification Report

TAXSAYA Online Version 1.5.0.12

File name: ISCB-5-RPT-C038-CR-v1a
Version: v1a
Date of document: 15 August 2013
Document classification: PUBLIC

Malaysian Common Criteria Evaluation & Certification Scheme®

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

Securing Our Cyberspace

CyberSecurity Malaysia
(726630-U)

T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C038 Certification Report

TAXSAYA Online Version 1.5.0.12

15 August 2013

ISCB Department

CyberSecurity Malaysia

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

Document Authorisation

DOCUMENT TITLE:	C038 Certification Report – TAXSAYA Online Version 1.5.0.12
DOCUMENT REFERENCE:	ISCB-5-RPT-C038-CR-v1a
ISSUE:	v1a
DATE:	15 August 2013

DISTRIBUTION:	UNCONTROLLED COPY – FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:
Level 5, Sapura@Mines,
No 7, Jalan Tasik,
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 15 August 2013, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement at www.commoncriteriaportal.org).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 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	1 August 2013	All	Final Release.
v1a	15 August 2013	Page iv	Add the date of the certificate.

Executive Summary

TAXSAYA Online Version 1.5.0.12 (hereafter referred as TAXSAYA) from EA Link System Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

TAXSAYA is a web application which is hosted by Microsoft Azure servers and it can be used by the users with Internet access via Internet Explorer or Firefox. Main functionality of the TOE is to assist Taxpayers to prepare and submit their Tax Returns.

TAXSAYA provides the following features to the authenticated users;

1. **User Interface Module**: This module provides the interface for identification and authentication of the client users, using username and password, in order to restrict the access to the TOE.
2. **e-Filing Module**: The e-Filing module manages the transfer of information into the e-Filing. Prior to the data being transferred, the user will be prompted to select the appropriate identification that has been registered with the LHDN, and to keyin the password. The TOE will then transfer all Assessment information into the e-Filing, and attempt to download the Draft e-Borang.
3. **Tax Wizard Module**: The Tax Wizard guides the tax preparer (user) through the process of gathering the Tax Information. While it allows the user to enter information in any order, it does perform basic data entry checks to ensure the validity of the individual elements provided. Before allowing the user to print/efile the final assessment information, the TOE will perform checks and issue warnings/errors to ensure consistency with the LHDN e-Filing. In addition, it will force the user to confirm and lock their tax number, as this is a critical piece of information.
4. **Reporting Module**: This module allows the user to print the final borang. In addition, the user can request the system to prepare a detailed report that itemises all the income and expense details that have been entered, to show how the figures in the Borang have been computed.

The administrative functions of the TOE such as backup, user management and others are handled by EA Link administrators through their accounts on Microsoft Azure Platform. However, this is outside the scope of evaluation.The functions of the TOE that are within the scope of evaluation covering:

- Audit logs generated for the auditable events,
- Identification and authentication of user before any action can be performed,
- Exporting user's tax data to E-Hasil portal, and
- Management of security attributes belong to the users.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with the evaluated configuration, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of the TOE to the Common Criteria (CC) Evaluation Assurance Level 1 (EAL1). The report confirms that 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 BAE Systems Detica evaluation facility (the 'BAE Systems Detica MySEF') and completed on 19 April 2013.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that TAXSAYA meets their requirements and security needs. It is recommended that a potential user of TAXSAYA 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 The Target of Evaluation (TOE), TAXSAYA Online Version 1.5.0.12 (hereafter referred as TAXSAYA) is a web application designed to assist tax payers to prepare and submit their tax returns. The TOE is hosted by Microsoft Azure servers and can be accessed via Internet Explorer or Firefox.

2 In order to restrict the access to the TOE, users are required to login using username and password. After successfully identified and authenticated, the users are prompted to provide necessary information in order to prepare their tax returns. TOE provides a tax wizard function to support users to fill all the required fields to complete the operation. A tax optimiser provides the Taxpayers with suggested tax savings. The final tax file can either be printed or automatically filed and upload to the Tax Department (E-Hasil).

3 The TOE can perform several operations within the user interface which includes; identification and authentication, calculation of tax returns, re-use tax data derived from previous year, produce paper base E-Hasil form (e-Borang), produce report for tax audit and tax optimization.

4 In the context of the evaluation, the TOE provides the following major security features; which will be discussed further in Section 1.4.1 of this document:

a) **Audit Logs** – TOE generates audit logs for the auditable events listed in section 5.1.1 of the Security Target (Ref [6]). These audit records can only be reviewed by TAXSAYA administrators. Audit review and actions taken according to the audit logs are outside the scope of this evaluation.

b) **Identification and Authentication** - TOE identifies and authenticates its users before any action. All registered users have a Username and Password in order to complete the identification and authentication process.

c) **Tax Data Export** – TOE provides a secure data export to the e-Hasil site by using the security attributes of the users. Users can upload their tax data to the e-Hasil site in order to complete the tax claim process.

d) **Management of Security Attributes** – TOE support the management of security attributes belong to the users such as Username, Password and IC Number. The management functions include:

i) Roles management

ii) Allow/deny access attempts

iii) Enforce access control policy

iv) Manage user session

1.2 TOE Identification

5 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	C038
TOE Name	TAXSAYA Online
TOE Version	Version 1.5.0.12
Security Target Title	TAXSAYA Online Version 1.5.0.12 Security Target
Security Target Version	Version 1.1
Security Target Date	7 February 2013
Assurance Level	Evaluation Assurance Level 1 (EAL1)
Criteria	Common Criteria for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL1
Sponsor and Developer	EA Link System Sdn Bhd, B2-05, Block B, 2nd Floor SME Technopreneur Centre Cyberjaya 2270, Jalan Usahawan 2 Cyberjaya, Selangor Tel: +603-8315 6020
Evaluation Facility	BAE Systems Detica MySEF

1.3 Security Policy

6 TAXSAYA implements Access Control Policy on exporting (upload) user tax data to the e-Hasil. Only user with valid IC number and e-Hasil password can upload their tax data to e-Hasil.

7 The details of the security policy are described in Section 4 and 5.1.3 of the Security Target (Ref [6]).

1.4 TOE Architecture

8 The TOE includes both logical and physical boundaries which are described in Section 2.2 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

9 The TOE implements and controls the security features listed below:

a) **Audit Logs**

The TOE generates audit log records via its Reporting Module for the auditable events listed in Table 4 of the ST (Ref [6]). These logs are stored on the Microsoft SQL database; which is outside the scope of the evaluation. Each audit log includes: the user who performs the operation, date and time of the event, type of the event, subject identity and outcome of the event. Audit log and actions taken according to the audit logs are outside the scope of the evaluation.

b) **Identification and Authentication**

Users are required to perform identification and authentication via User Interface Module before any actions on the TOE are permitted. Users can generate their own username and password according to a defined metric enforced which checks the password if it contains at least three of the following requirements:

i. Lower case characters,

ii. Upper case characters,

iii. Numbers,

iv. Symbols.

The TOE enforce the users to setup the password between 6 to 16 characters. New password can be generated upon request by the user. The TOE also maintains IC Number as well as the username and password for each user for authentication to the E-Hasil site during data export.

An account will be locked for 24 hours if the authentication attempt fails for 3 times.

c) **Tax data export**

Users can upload their tax data to the e-Hasil by using the e-Filing module of the TOE. The TOE will enforce an access control policy during data export. Only the authorised users with a valid IC Number and e-Hasil password can upload their tax data to e-Hasil.

d) **Management of Security Attributes**

The TOE provides a management interface that allows the users to manage the security attributes belong to the users as follows:

i. Username

ii. Password

iii. IC Number

1.4.2 Physical Boundaries

10 Figure 1 below describes the typical installation of TAXSAYA which consists of the TOE.

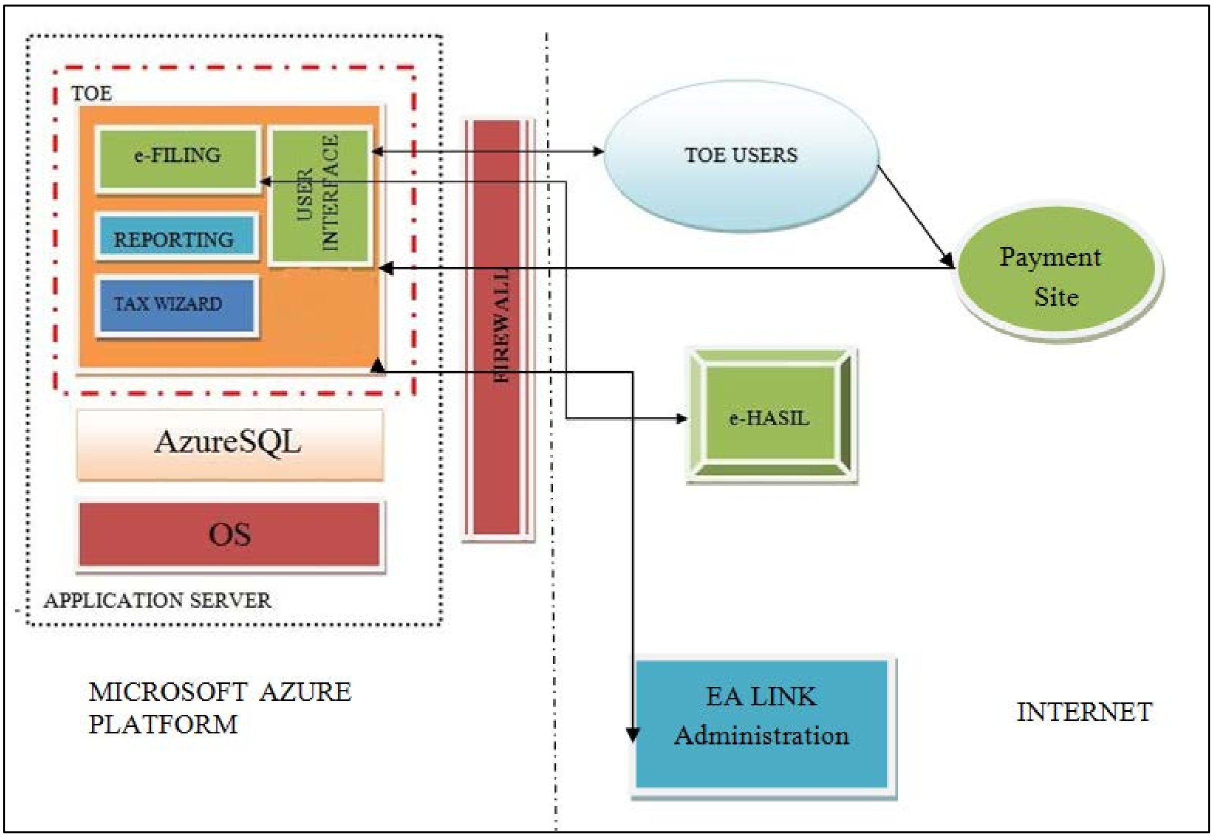

Figure 1: TOE Physical Scope

11 The TOE is installed in an application server and providing its service to its users through an internet connection. A virtual machine is hosting the application prepared by EA Link on Microsoft Azure platform. The platform, virtual machine, SQL server and interface to the vendor for maintaining the system are outside the scope of TOE.

12 The TOE provides the following features to the authenticated users:

a) User Interface Module – This module provides identification and authentication of the users in order to restrict the access to the TOE. The users who request a service from the TOE is enforced to provide a valid username and password. If the username and password is incorrect, the user is not allowed to access to the TOE and its resources. This module is also providing the communication between authorised users and TOE modules.

b) e-Filing Module – The e-Filing module manages the transfer of information into the e-Filing. Prior to the data being transferred, the user will be prompted to select the appropriate identification that has been registered with the LHDN, and to key in the password. The TOE will then transfer all assessment information into the e-Filing, and attempt to download the draft e-Borang.

c) Tax Wizard Module - The Tax Wizard guides the user through the process of gathering the tax information. While it allows the user to enter information in any order, it does perform basic data entry checks to ensure the validity of the individual elements provided. Before allowing the user to print/efile the final assessment information, the TOE will perform checks and issue warnings/errors to ensure consistency with the LHDN e-Filing. In addition, it will force the user to confirm and lock their tax number, as this is a critical piece of information.

d) Reporting Module - This module allows the user to print the final e-Borang. In addition, the user can request the system to prepare a detailed report that itemises all the income and expense details that have been entered, to show how the figures in the e-Borang have been computed.

13 The TOE is a web application that relies on supporting hardware and software as described in Section 2.1 of the Security Target (Ref [6]).

14 The Security Target assumes that environment provides appropriate physical security for the TOE. This would restrict direct access to the TOE.

1.5 Clarification of Scope

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

16 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]).

17 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.

18 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 configured with IIS and .NET 4.0;

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

d) User computer which includes the operating system, internet browser etc;

e) User registration, account generation and account activation process to use the TOE;

f) Administrative functions of the TOE such as back up, maintenance of software etc; and

g) Audit review and action taken according to the audit logs.

1.6 Assumptions

19 There is no assumption declared by developer.

1.7 Evaluated Configuration

20 The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented user guidance (Ref [24]) and defined in Section 2.2 of the Security Target (Ref [6]).

1.8 Delivery Procedures

21 The TOE is a web based application, therefore to use the application, user need to complete an online registration and then will be directed to payment gateway to pay the service fee before being able to use the TOE.

22 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

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

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

a) TAXSAYA Online Core, Guidance Documentation, v3.0, April 2013.

2 Evaluation

25 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

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

2.1.1 Life-cycle support

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

2.1.2 Development

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

2.1.3 Guidance documents

29 The evaluators examined the TOE preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

30 Testing at EAL1 consists of performing independent function test, and performing penetration tests. The TOE testing was conducted at BAE Systems Detica MySEF lab in Plaza Sentral, Kuala Lumpur. 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

31 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.

32 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 as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
To test that the TOE authenticate each user before allowing any other TSF-mediated actions on behalf of that user	FIA_UAU.2 User authentication before any action	• User interface with User interface module. • Interface between TOE and Azure SQL. • Interface between TOE and iPay88 site.	**PASS.**
To test that the TOE identified each user before allowing any other TSF-mediated actions on behalf of that user	FIA_UID.2 User identification before any action	• Interface between TOE and AzureSQL. • User interface with user interface module.	**PASS.**

To test that the TOE detect three unsuccessful authentication attempts occur related to the user authentication during log-on. If the number has been met, the TOE must lock user account.	FIA_AFL.1 Authentication Failure Handling	Interface between TOE and AzureSQL.	**PASS.**
To test that the TOE provide mechanism to verify that secrets meet min 6-max 16 characters, check for three out of four requirements lower, upper case, numbers and symbols.	FIA_SOS.1 Verification of secrets	User interface with user interface module.	**PASS.**
To test the TOE capable of performing the following management functions: [changing user password]	FMT_SMF.1 Specification of Management Functions	User interface with user interface module	**PASS.**
1. To test that the TOE maintain the roles [users]. 2. To test that the TOE able to associate users with the roles.	FMT_SMR.1 Security Roles	User interface with user interface module	**PASS.**
To test if the TOE maintain following attributes belonging to individual users [username, password, IC Number]	FIA_ATD.1 User Attribute Definition	Interface between TOE and AzureSQL.	**PASS.**
To test that the TOE enforces the data export access control policy when exporting user data.	FDP_ETC.2 Export of user data with security attributes	• Interface between TOE and Active X. • User interface with Tax Agent module.	**PASS.**

To test that the TOE enforce the data export access control policy on a) authorised users Objects: a) tax data Operations: a) upload objects to e-Hasil	FDP_ACC.1 subset access control	• Interface between TOE and Active X. • User interface with assessment module. • User interface with e-filling manager.	**PASS.**
1) To test that the TOE enforce the data export access control policy to objects based on the following: a) Object (Authorised Users) b) subject (Tax Data) c) security attributes (user name, password, IC number) 2) The data export access control policy will only allow the operation if it [the IC number and e-Hasil password of the user is correct at the e-Hasil site] 3) To test the TOE explicitly authorise access of subjects to objects without additional rules 4) To test that the TOE explicitly deny access of subjects to objects without additional rules	FDP_ACF.1.1 FDP_ACF.1.2 FDP_ACF.1.3 FDP_ACF.1.4 Security attribute based access control	• Interface between TOE and Active X. • User interface with assessment module. • User interface with e-filling manager.	**PASS.**
To test that the TOE enforce the data export access control policy to restrict the ability to upload tax data to e-Hasil the security attributes username, password, IC Number to users.	FMT_MSA.1 Management of security attributes	User interface with user interface module.	**PASS.**

To test that the TOE enforce the data export access control policy to provide permissive default values for security attributes that are used to enforce the SFP. Also to test that TSF only allow users to specify alternative initial values to override the default values when an object or information is created.	FMT_MSA.3 Static attribute initialisation	User interface with user interface module.	**PASS.**
To test that the TOE generates audit record for: - start up and shutdown of the audit functions - all auditable events for the basic level of audit And within each of those audit record at least following information is included - date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event	FAU_GEN.1 Audit data generation	• User interface with user interface module • User interface with assessment module • User interface with e-filling manager • Interface between TOE and AzureSQL	**PASS.**

To test that the TOE able to associate each auditable event to a user that caused the event	FAU_GEN.2 User identity association	• User interface with user interface module • User interface with assessment module • User interface with e-filling manager • Interface between TOE and AzureSQL	**PASS.**

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

2.1.4.2 Penetration Testing

34 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE and to determine whether these were exploitable in the intended operating environment of the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, and functional specification.

35 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE, in its operational environment, is resistant to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during penetration tests:

a) Time taken to identify and exploit (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.

36 The penetration tests focused on:

a) Injection attacks;

b) Security misconfiguration; and

c) Information disclosure.

37 The results of the penetration testing note that there is no exploitable vulnerability 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

38 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

39 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

40 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 TAXSAYA performed by the BAE Systems Detica MySEF.

41 The BAE Systems Detica MySEF found that TAXSAYA 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.

42 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities 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

43 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.

44 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.

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

3.2 Recommendation

46 In addition to ensure secure usage of the product, below are additional recommendations for TAXSAYA consumers:

a) The users of the TOE should make themselves familiar with the user guidance provided with the TOE and pay attention to all security warnings.

b) All SSL certificates are maintained and valid (not revoked or expired), and are sourced from a trusted entity.

c) Use the product 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] TAXSAYA Online Version 1.5.0.12 Security Target, Version 1.1, 7 February 2013.

[7] EAL1 Evaluation Technical Report TAXSAYA, Version 1.0, 19 April 2013

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
EAL	Evaluation Assurance Level
IEC	International Electrotechnical Commission
ISCB	Information Security Certification Body
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

Acronym	Expanded Term
TOE	Target of Evaluation
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Access Control Policy	The security policy of the TOE which controls access from controlled subjects.
Borang	A paper based tax form prescribed by the Malaysian Tax Department
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.
e-Borang	An electronic tax form provided by the Malaysian Tax Department for the purpose of submitting tax online.
EA Link Administrator	Users which maintain TOE through Microsoft Azure interface provided by Microsoft.
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.

Term	Definition and Source
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 ---