C017 Certification Report
BT-Direct Version 2010.1.0.0

File name: ISCB-5-RPT-C017-CR-v1a
Version: v1a

Date of document: 25 May 2011

Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 8, Block A
Mines Waterfront Business Park
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8946 0999
F +603 8946 0888
www.cybersecurity.my

C017 Certification Report

BT-Direct Version 2010.1.0.0

25 May 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:	C017 Certification Report - BT-Direct Version 2010.1.0.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C017-CR-v1a
ISSUE:	v1a
DATE:	25 May 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 25 May 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	16 May 2011	All	Final Released.
v1a	25 May 2011	Page iv	Add the date of the certificate.

Executive Summary

BT-Direct version 2010.1.0.0 (hereafter referred as BT-Direct) from EA Link System Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

BT-Direct is an electronic tax submission software designed for Malaysian Tax Agents in order to do e-Filing using the Tax Agent e-Filing (TAeF) sign on and also to conduct Tax Payer's e-Filing on behalf of their clients.

The security features within the scope of the Security Target (ST) includes:

- **Audit Function** – BT-Direct generate audit logs in order to follow up the audit trails and system events. Only authorised users can access the audit logs.
- **Data Protection** – Access to the TOE features and data are subject to access control policy.
- **Identification and Authentication** – Users of BT-Direct can access to the TOE after a successfully logging in based on their user ID and password.
- **Security Management** – The security functions of BT-Direct can be managed either by BT-Direct or the authorised users. BT-Direct can manage access control within the scope of the policies according to the assigned access rights and defined user credentials by the administrator.

The scope of the evaluation is a subset of the BT-Direct System. The Active X Controls, Security Wrapper, DBISAM Database and the communication interface with the e-Hasil system (Inland Revenue Board of Malaysia's electronic Income Tax Return Form (ITRF) filing system), Windows Operating System and Internet Explorer application are part of the IT environment and not in the 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 BT-Direct, 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 describes the findings of the IT security evaluation of BT-Direct, to the Common Criteria (CC) evaluation assurance level of EAL 1 and that the evaluation was conducted in accordance with relevant criteria and the requirements of the Malaysia's Common Criteria Certification (MyCC) Scheme. The evaluation was performed by CyberSecurity Malaysia Security Evaluation Facilities (MySEF). The evaluation was performed by the CyberSecurity Malaysia MySEF and was completed on 19 November 2010.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the BT-Direct 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 BT-Direct meet their requirement and security needs. It is recommended that prospective users of the BT-Direct 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 Target of Evaluation (TOE), BT-Direct version 2010.1.0.0 (hereafter referred as BT-Direct) is an electronic tax submission software designed for Malaysian Tax Agents in order to do e-Filing using the Tax Agent e-Filing (TAeF) sign on and also to conduct Tax Payer's e-Filing on behalf of their clients. It is an interface between the user and the e-Hasil system (Inland Revenue Board of Malaysia's electronic Income Tax Return Form (ITRF) filing system), where the users can perform all of e-Filing operations.

2 BT-Direct System can be used within a network and with multiple users in order to conduct e-Filing operations by importing tax assessment data from Brasstax Database or XML files. These inputs are going to be imported into the TOE and validated. The validated data is exported to the e-Hasil system by an e-Filing Manager using Internet Explorer Active X Controls.

3 The TOE consists of the following five main modules and requires internet connection to export the data to the e-Hasil system;

a) Import Module

b) User Management Module

c) Tax Agent Module

d) Assessment Module

e) e-Filing Manager

4 The security features within the scope of the Security Target (ST) includes:

a) **Audit Function** – BT-Direct generate audit logs in order to follow up the audit trails and system events. Only authorised users can access the audit logs.

b) **Data Protection** – Access to the TOE features and data are subject to access control policy.

c) **Identification and Authentication** – Users of BT-Direct can access to the TOE after successfully logging in.

d) **Security Management** – The security functions of BT-Direct can be managed either by BT-Direct or the authorised users. BT-Direct can manage access control within the scope of the policies according to the assigned access rights and defined user credentials by the administrator.

1.2 TOE Identification

5 The details of the TOE are identified in Table 1 below.

Table 1: TOE Identification

Scheme	Malaysian Common Criteria Evaluation and Certification

	(MyCC) Scheme
Project Identifier	C017
TOE Name`	BT-Direct
TOE Version	version 2010.1.0.0
Security Target Title	BT-Direct Version 2010.1.0.0 SECURITY TARGET
Security Target Version	v2.1
Security Target Date	18 November 2010
Assurance Level	Evaluation Assurance Level 1 (EAL1)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL1
Sponsor and Developer	EA Link System Sdn Bhd B2-05, Block B, 2nd Floor, SME Technopreneur Centre Cyberjaya, 2270 Jalan Usahawan 2, 6300 Cyberjaya, Selangor MALAYSIA
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

6 In order to provide user data protection, BT-Direct implements access control policy where only authorised users will be granted access to the data, including import of user data and export of the Tax Profile to the e-Hasil, based on their associated security group. The main security groups introduced in the operational user guidance are Administrators, Tax Manager and Staff. The users are associated to a specific role and conduct the permitted operations. The access control policy is enforcing the authorisations of the users and denies the access requests to the objects that are not allowed.

7 The detail of the access control policy is described in Section 4.2 and Section 5 of the Security Target (Ref [6]).

1.4 TOE Architecture

8 BT-Direct Security Target defines clearly both logical and physical boundaries.

9 Figure 1 illustrates the architecture of the TOE logical boundary in terms of modules.

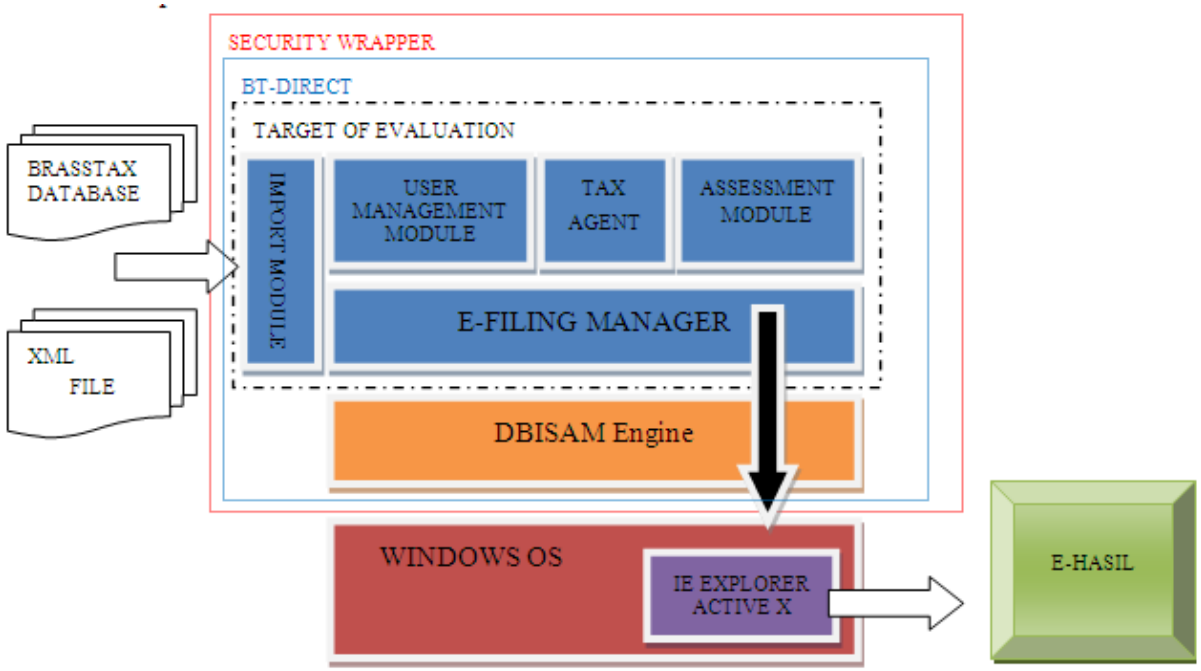

Figure 1: TOE boundary & TOE subsystems (logical view)

10 The TOE consists of five modules as described below:

a) **Import Module**: This module performs the importing of the tax assessment data from the source system. During the import process, the TOE will enforce all data type checking and validation rules that will be enforced in the e-Filing. These rules are pulled from an XML file which defines the schema for the particular Tax Data being imported. Currently, imports from XML and BRASSTAX sources are supported, however these may be expanded in time to support additional data formats e.g. PDF and Excel. During the importing, it is necessary for the user to define both the User and the Tax Agent that is assigned to the Assessment. The Assignment of the user, can define which Assessments the user can see when they access the assessment list, while the Tax Agent Assignment will control the ID that will be used when transferring the Assessment details into the e-Filing. Upon successful import of an assessment, the relevant information will be logged into the Audit file.

b) **User Management Module**: This module allows the administrator to define and administer authorised users of the TOE, and allows authorised users to change their passwords. The functionality given to administrators allows them to define security profiles in the form of user groups and to assign them to individual users. In addition, administrators also have the ability to lock (or bar) individual users from accessing the TOE. Each successful change

will trigger an update in the Audit file to reflect the operation that was performed.

c) **Tax Agent Module**: The Tax Agent module allows the administrator to define how the TOE will sign on into the TAeF (Tax Agent e-Filing Module). Each authorised users defined in the TAeF will have a user ID and can in turn be assigned to a given Assessment. The Tax Agent information defined in the TOE should match exactly with which is defined in the TAeF. Each time the details in the Tax Agent module are changed, an entry will be made into the Audit log.

d) **Assessment Module**: This module is used by authorised users for assessing the imported e-Borang data before sending to e-Hasil. The basic operations are to create, update, delete and open assessment. It also allows user to look at their profiles and provides the necessary user interfaces to allow the authorised user to initiate the sending of Assessment data into the TOE. This module enforces the rules that determine what operations are permitted according to the state of the Assessment (where the state of the Assessment is changed following the successful completion of each e-Filing activity). The Security Profile and the Assignment of the Assessments can control which assessments can be seen here.

e) **e-Filing Manager**: This module is the interface that manages the communication between TOE and the e-Hasil system. This module performs the necessary operation for sending the Assessment data to e-Hasil. There are 6 major functions as follows:

i. Register - register the Borang with the TAeF using the assigned Tax Agent information (as defined in the Tax Agent Module). If the Tax Number has not been previously assigned, the authorised user will be asked to confirm the assignment.

ii. Load - transfer all assessment information from the TOE into the TAeF.

iii. Draft - request the draft e-Borang from the TAeF for the current Assessment.

iv. Approve - this function is not an e-Filing function. It performs the task of managing the process control, by disabling the register and load functionalities, and unlocking the sign function.

v. Sign - allow the user to confirm the assessment in the TAeF, and will apply the Taxpayer's digital signature. Once this function is performed, the system will attempt to download the final e-Borang and the Acknowledgement. Once this function is performed, the authorised user may only request the final documents.

vi. Final - download the final e-Borang and the Acknowledgement form from the TAeF.

Each of the above e-Filing operations will cause the state of Assessment to be changed, and an entry will be made into the Audit Trail to reflect the operation that was performed.

1.5 Clarification of Scope

11 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) **Audit Function**: In order to follow up the audit trails and system events the TOE generate audit logs and only authorized users can access the audit logs. Import Module, User Management Module, Tax Agent Module, Assessment Module and e-Filing Manager calls Audit Function in various events defined in table below:

Table 2: Auditable event

SUBJECT	OBJECT	EVENT
Any User	Identification Mechanism	Successful Login
Any User	Identification Mechanism	Unsuccessful Login Attempt
Administrator	User Management Module	Add, Delete, Modify User/Security Group
e-Filing Manager	User Data	Register, Load, Approve, Sign Assessment
Administrator, Tax Manager, Staff	Assessment	Assessment is imported or deleted.

The audit function will start to generate audit logs when the system starts and will stop generating logs when the system closed. The start-up and shut down of the system and the audit functionality is also logged in the license server.

The TOE receives the time stamps from the operating system and record time for the audited events.

b) **Data Protection**: providing the capability to the TOE for implementing an access control for the authorised users according to their associated security group. Data Protection Function controls functions in Import Module and e-Filing Manager.

The users are associated to a specific role and conduct the permitted operations. The Access control policy is enforcing the authorisations of the users and denies the access requests to the objects that is not allowed.

c) **Identification and Authentication**: The users of the TOE can access to the TOE after a successfully logging in. Identification and Authentication Function is related with User Management Module.

Authentication fails when the defined value (3) of the unsuccessful attempts has been met. The associated user account will be locked for 24 hours and become unavailable. After 24 hours the account will be available automatically or the user can apply to the administrator for a prior status change.

d) **Security Management**: The security functions of the TOE can be managed either by the TOE or the authorised users of the TOE. The TOE can manage access control within the scope of the policies according to the assigned access rights and defined user credentials by the administrator.

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 in the scope of the evaluation, but these IT environment are required to ensure that the TOE perform in its intended operations, are as follows:

a) Operating system, internet explorer, Adobe Acrobat Reader, License Server, e-Hasil, Active X Controls.

b) The security wrapper (Remote IP Server), which check the validity of the license credentials which may be stored locally or remotely.

c) The DBISAM database application where the TOE store and process the user data.

1.6 Assumptions

14 This section summarises the security aspects of the environment or configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and what is required for secure operation of the BT-Direct as defined in the Security Target (Ref [6]). Consumers can make informed decisions about the risks associated with using the BT-Direct by considering assumptions about usage and environment settings as requirements for the product's installation and its operating environment, to ensure its proper and secure operation.

15 However, there is no assumption declared in the Security Target and the specific item needs by the TOE was explained in Section 3.1 Security Objective for the Operational Environment of the Security Target.

1.7 Evaluated Configuration

16 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 installation guide (Ref 27a)).

17 The TOE user is responsible to configure the TOE based on the installation guide (Ref 27a)). The installation will be done in 3 steps:

a) Data Server Installation (BTDirect2010v100Setup.exe) downloadable from www.ealink.com

b) License Server Installation (BTDirect2010Licensesetup.exe). The setup file is copied onto the Data Server machine during the installation of the Data Server.

c) Client Workstation Installation (BTDirect2010ClientSetup.exe). The setup file is copied onto the Data Server machine during the installation of the Data Server. The Client Workstation installation must be run on every PC that is going to access BTDirect2010.

18 The TOE is installed to the workstations within a local area network. The hardware including workstation, network infrastructure, monitor, I/O devices, disk drives and the softwares including the operating system, internet explorer, Adobe Acrobat Reader, DBISAM Database, License Server, Security Wrapper, e-Hasil, and Active X Controls. These components are IT environment which helps TOE to perform in its intended operations.

19 Figure 2 shows the generic BT-Direct system architecture which can be installed according to the installation guide provided to the user.

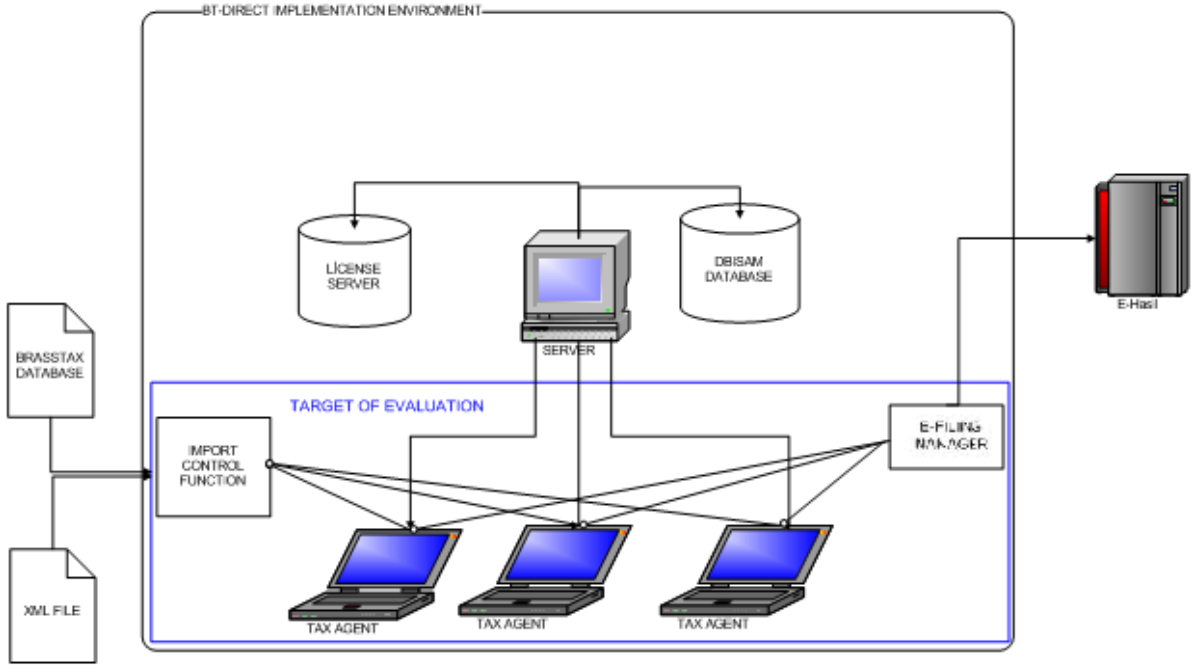

Figure 2: General BT-Direct System Architecture

20 The TOE is installed to the Tax Agent's computer in the above figure. All Tax Agents' computer, which installed with the TOE, will communicate with e-Hasil using Internet connection through e-Filing Manager.

21 The communication with e-Hasil is provided by the LHDN infrastructure. Currently, https is used for the secure communication.

1.8 Delivery Procedures

22 BT-Direct and its guidance documentations can be downloaded from the developer's website at www.ealink.com.

23 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus the evaluators did not verify any TOE delivery process.

24 In Section 3.1 Security Objectives of the Operational Environment in the Security Target, OE.INSTALL stated the trusted users must install the TOE according to the preparative user guidance provided with the software. Therefore, the evaluators relied on the environment to provide a secure TOE delivery process.

1.9 Documentation

25 It is important that the BT-Direct is used in accordance with guidance documentation in order to ensure secure usage of the product.

26 The following guidance software is provided by the developer to the end user as guidance to ensure secure usage and operation of the product:

a) BTDirect 2010 Help Guide (software), v1.1.0

b) BT Direct 2010 Help File (video)

27 The following guidance document and software are provided by the developer that the user can use as guidance for secure installation of the product:

a) BT Direct 2010 Installation Guide (Ref [8])

b) BTDirect 2010 Help Guide (software), v1.1.0

c) BT Direct 2010 Help File (video)

2 Evaluation

28 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

29 The evaluation activities involved a structured evaluation of BT-Direct, including the following components:

2.1.1 Life-cycle support

30 An analysis of the BT-Direct 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

31 The evaluators analysed the BT-Direct 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

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

2.1.4 IT Product Testing

33 Testing at EAL1 consists of performing independent function test, and performing penetration tests. BT-Direct testing was conducted by CyberSecurity Malaysia MySEF at CyberSecurity Malaysia MySEF Lab in 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 Independent Functional Testing

34 At EAL1, independent functional testing is 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.

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

Table 3: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	STATUS
This test group verifies the audit trails and system events the TOE generate audit logs and only authorized users can access the audit logs. Import Module, User Management Module, Tax Agent Module, Assessment Module and e-Filing Manager calls Audit Function in various events defined in ST.	Security Audit	• Interface Between TOE and DBISAM • User Interface with User Management Module • User Interface with Assessment Module • User Interface with e-Filing Manager	PASS. The output shows that the TOE functions as per claims.
This test group verifies the TOE features and data are subject to access control and the operations conducted within the TOE are subject to information flow control. Data Protection Function controls functions in Import Module and e-Filing Manager.	User Data Protection	• Interface Between TOE and XML/ BrassTax File • Interface Between TOE and Active X • User Interface with User Management	PASS. The output shows that the TOE functions as per claims.

DESCRIPTION	SECURITY FUNCTION	TSFI	STATUS
		Module • User Interface with Tax Agent Module • User Interface with Assessment Module • User Interface with e-Filing Manager	
This test group verifies the TOE can access to the TOE after a successfully logging in. Identification and Authentication Function is related with User Management Module.	Identification and Authentication	• Interface Between TOE and DBISAM • User Interface with User Management Module	PASS. The output shows that the TOE functions as per claims.
This test group verifies the TOE can be managed either by the TOE or the authorised users of the TOE. The TOE can manage the access control and information flow control within the scope of the policies according to the assigned access rights and defined user credentials by the administrator. Addition to the above functions, the Operational Environment for	Security Management	• User Interface with User Management Module	PASS. The output shows that the TOE functions as per claims.

DESCRIPTION	SECURITY FUNCTION	TSFI	STATUS
the TOE provides time stamps for the audit logs.			

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

2.1.4.2 Penetration Testing

37 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.

38 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.

39 The penetration tests focused on :

a) Generic vulnerabilities;

b) Direct attack.

40 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment.

2.1.4.3 Testing Results

41 Tests conducted for the BT-Direct produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

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

3 Results of the Evaluation

43 After due consideration during the oversight of the evaluation execution by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of BT-Direct performed by CyberSecurity Malaysia MySEF.

44 CyberSecurity Malaysia MySEF found that BT-Direct 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.

45 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

46 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.

47 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.

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

3.2 Recommendation

49 In addition to ensure secure usage of the product, below are additional recommendations for BT-Direct:

a) Encrypt user credential using strong encryption algorithm before it is stored in the DBISAM server.

b) Underlying hardware, software and network should be hardened. All access to the administrator interfaces and the underlying OS should be restricted to trusted users only.

c) The users must be well trained to ensure that they will only use the TOE in secure manner according to the secure operational user guidance.

d) 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] BT-Direct Version 2010.1.0.0 SECURITY TARGET, version 2.1, 18 November 2010.

[7] Evaluation Technical Report BT-Direct Version 2010.1.0.0, version 1, 19 November 2010.

[8] BT Direct 2010 Installation Guide, v2010.1.2, 25 October 2010.

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology (ISO/IEC 18045)
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
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

Acronym	Expanded Term
ST	Security Target
TAeF	Tax Agent e-Filing Module
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 5: 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.
e-Borang	An electronic tax form provided by the Inland Revenue Board Of Malaysia for the purpose of submitting tax online.
e-Filing	Inland Revenue Board Of Malaysia's online application on filing Income Tax Return Form (ITRF) electronically through internet for the following Forms: Form B - Business Income Form BE - Non-Business Income Form P - Partnership Form M (e-M) - Non-resident Individual Form E (e-E) - Employer Form C (e-C) - Company Form R (e-R) - 108 statement for company e-Estimated (e-CP204) - An online Estimate Tax Payable Form submission for Company/Co-operative Society/Trust Body
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.
Tax Agent e-Filing Module (TAeF)	e-Filing system for Tax Agents to file Income Tax Return Forms electronically on behalf of the clients. Can be accessed via the website at https://e.hasil.gov.my.

--- END OF DOCUMENT ---