The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

EA LINK SYSTEM SDN BHD

BT-DIRECT
COMMON CRITERIA
EAL1 CERTIFICATION

BT-Direct Version 2010.1.0.0

SECURITY TARGET v2.1

Version No	2.1		
Release Date	18/11/2010		
Document Code	E020-ST-2.1		
File Name	E020-ST-2.1.DOCX	**Language**	ENGLISH
Project	BT-DIRECT COMMON CRITERIA EAL1 EVALUATION PROJECT		
Title	BT-DIRECT Version 2010.1.0.0 SECURITY TARGET 2.1		
Category	DELIVERABLE		
Prepared By	FIRMUS SECURITY SDN BHD		

Version History

Version No	Reason for Change	Release Date
0.1	First Release	14/04/2010
0.2	Developer Comments	15/04/2010
0.3	Consultant Review and Update	22/04/2010
0.4	First Submission to MySEF	23/04/2010
0.5	Revised with comments from MySEF	30/04/2010
0.6	Additional SFR to the IT Environment	13/05/2010
1.0	Preparation of v1.0 after ERR #001 from MySEF	25/05/2010
1.1	Preparation of v1.1 after ERR #002 from MySEF	14/06/2010
1.2	Update for the EPP	25/06/2010
1.3	Updated TOE name to BT-Direct, version 2010 and added Import Module	09/07/2010
1.4	Removed “International Standard” under Section 1.1 Defined “Borang” and “e-Borang” under Section 1.3.2 Terminology Updated Security Management under Section 2.3TOE Security Features	20/07/2010
1.5	Revised after EOR #001 from MySEF	05/08/2010
1.6	Revised after EOR #001 (re-issued) from MySEF	18/08/2010
1.7	Revised after EOR #001 (re-issued) and EOR #003 from MySEF	08/09/2010
1.8	Revised after EOR #003 d1a from MySEF	18/10/2010
1.9	Revised after a meeting with CSM	29/10/2010
2.0	Update in the Security Functional Requirements	03/11/2010
2.1	Update in the Security Objectives after Vulnerability Assessment	18/11/2010

Approvals

Name	Role	Date
Mehmet ÇAKIR	ST Author (Firmus Security Sdn Bhd)	
Shang Ye WAI	ST Author (Firmus Security Sdn Bhd)	
Eric YEOW	Vice President (Firmus Security Sdn Bhd)	
Trevor KEEGAN	Managing Director (EA Link System Sdn Bhd)	

Primary Recipients

Name	Role	Date
Wan Shafiuddin ZAINUDIN	Senior Evaluator	

Comments

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

CONTENT

1 ST INTRODUCTION 7

1.1 Security Target, TOE, Common Criteria Identificaton 7
1.2 CC Conformance Claim 7
1.3 Conventions, Terminology, Acronyms 7
1.4 ST Overview and Organization 8

2 TOE OVERVIEW 8

2.1 TOE Type 10
2.2 TOE Description 10
2.3 TOE Security Features 12

3 SECURITY OBJECTIVES 14

3.1 Security Objectives For The Operational Environment 14

4 IT SECURITY REQUIREMENTS 15

4.1 Extended Components Definition 15
4.2 TOE Security Functional Requirements (SFRs) 15
4.3 TOE Assurance Requirements (SARs) 20

5 TOE SUMMARY SPECIFICATIONS 20

5.1 TOE Security Functions 20

APPENDIX A ACRONYM LIST 23

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

INDEX OF TABLES

Table 1 Security Objectives for the Operational Environment 14
Table 2 Security Functional Requirements 16
Table 3 Audited Events 16
Table 4 Security Assurance Requirements.....20
Table 5 Auditable Event Details 21
Table 6 Acronyms List.....23

INDEX OF FIGURES

Figure 1 General BT-Direct System Architecture 9
Figure 2 Logical Boundaries of the TOE 11

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

1 ST INTRODUCTION

This section presents the following information:

- Identifies the Security Target (ST) and Target of Evaluation (TOE);
- Specifies the ST conventions and ST conformance claims; and,
- Describes the ST organization.

1.1 Security Target, TOE, Common Criteria Identificaton

ST Title : BT-Direct Version 2010.1.0.0 SECURITY TARGET

ST Version : 2.1

TOE Software Identification : BT-Direct **Version 2010.1.0.0**

Evaluation Assurance Level : EAL 1

CC Identification : CC for Information Technology (IT) Security Evaluation, Version 3.1, Revision 3, July 2009 (CCMB-2009-07-001, CCMB-2009-07-002, CCMB-2009-07-003)

Keywords : BrassTax, Tax, e-Borang, e-Filing, e-Hasil, LHDN, IRB, Malaysia, MyCC, MyCB, MySEF, Common Criteria, Common Evaluation Methodology, Evaluation Assurance Level, Information Security.

1.2 CC Conformance Claim

This TOE and ST are consistent with the following specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, Revision 3, July 2009, extended.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements Version 3.1, Revision 3, July 2009, conformant, EAL1.

This ST makes no conformance claims to any certified Protection Profile.

1.3 Conventions, Terminology, Acronyms

This section specifies the formatting information used in the ST.

1.3.1 Conventions

In this Security Target some notations and conventions which are taken from the Common Criteria v3.1R3 have been used in order to guide to the reader.

During the specification of the functional requirements under the Section 4, the functional components are interpreted according to the “assignment” and “selection” operations.

The outcome of the assignment operations are shown with **bold** and identified between “[**brackets**]”.

The outcome of the selection operations are shown with **bold** and **underlined** and identified between “[**brackets**]”.

1.3.2 Terminology

The following terminology is used in this Security Target:

Access Control Policy: The enforcements of the TOE where the users are subject to before conducting actions.

Administrator: An authorized user which has specified privilages in order to manage and maintain the TOE.

Tax Manager: A person with the necessary knowledge and experience to oversee, check and approve the work of staff.

Staff: Any person working in the Tax firm responsible for performing one or more tasks relating to an assigned client tax assessment.

Authorized User: A Human User that has been properly identified and authenticated.

Borang: A paper based tax form prescribed by the Malaysian Tax Department.

e-Borang: An electronic tax form provided by the Malaysian Tax Department for the purpose of submitting tax online.

1.3.3 Acronyms

The acronyms used in this ST are specified in Appendix A – Acronym List.

1.4 ST Overview and Organization

This Security Target is consist of five sections and an Appendix. The reader could find out the following definition in these sections;

- Section 1 – Security Target Introduction: The unique references for the TOE and for the ST including the document conventions, terminology and the acronyms.
- Section 2 – TOE Description: Provides an overview to the TOE and its IT Environment.
- Section 3 – Security Objectives: Defines the security objectives for the IT Environment for the secure usage of the TOE.
- Section 4 – IT Security Requirements: The functional and assurance requirements of the TOE claimed by the developer.
- Section 5 – TOE Summary Specifications: Defines the security functions provided by the TOE in order to satisfy the security requirements.
- Appendix A: The acronyms used inside the security Target.

2 TOE OVERVIEW

The Target of Evaluation is designed for Malaysian Tax Agents in order to do e-Filing using the Tax Agent e-Filing (TAeF) sign on and also for them in order to conduct Tax Payer's e-Filing on behalf of their clients.

BT-Direct can also be installed and used with a free license which is not subject to an evaluation and the difference between licenses would be clearly stated to the users in order to avoid from possible ambiguities.

The physical and logical boundaries and the IT environment of the TOE is defined in the Section 2.3 where the reader of this Security Target can be able to understand the scope of the certification.

For a complete definition of the TOE, this section will first cover the description and the features of BT-Direct.

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 system and validated. The validated data is sent to the e-Hasil system by an e-Filing Manager. The export of data to the e-Hasil is performed by utilising Internet Explorer Active X Controls.

The users of the BT-Direct can be able to perform the following operations with their user interface;

- Register Borang
- Request for Draft e-Borang
- Sign e-Borang
- Request for Acknowledgement
- Auto Update of TAeF status
- Batch Loading
- Batch Request for Draft
- Auto login to TAeF
- Auto loading of e-Borang

- Error image control
- Import from Brasstax Database
- Import from XML file

The administrator of the BT-Direct can be able to perform the following operations with the user interface;

- Security setup
- Create Users and compose access rights
- Assignment of assessment data to authorized users
- Audit trail control
- Database Maintenance

The following figure is showing the General BT-Direct system architecture which can be installed according to the preparative user guidance provided to the user enclosed to the BT-Direct Software.

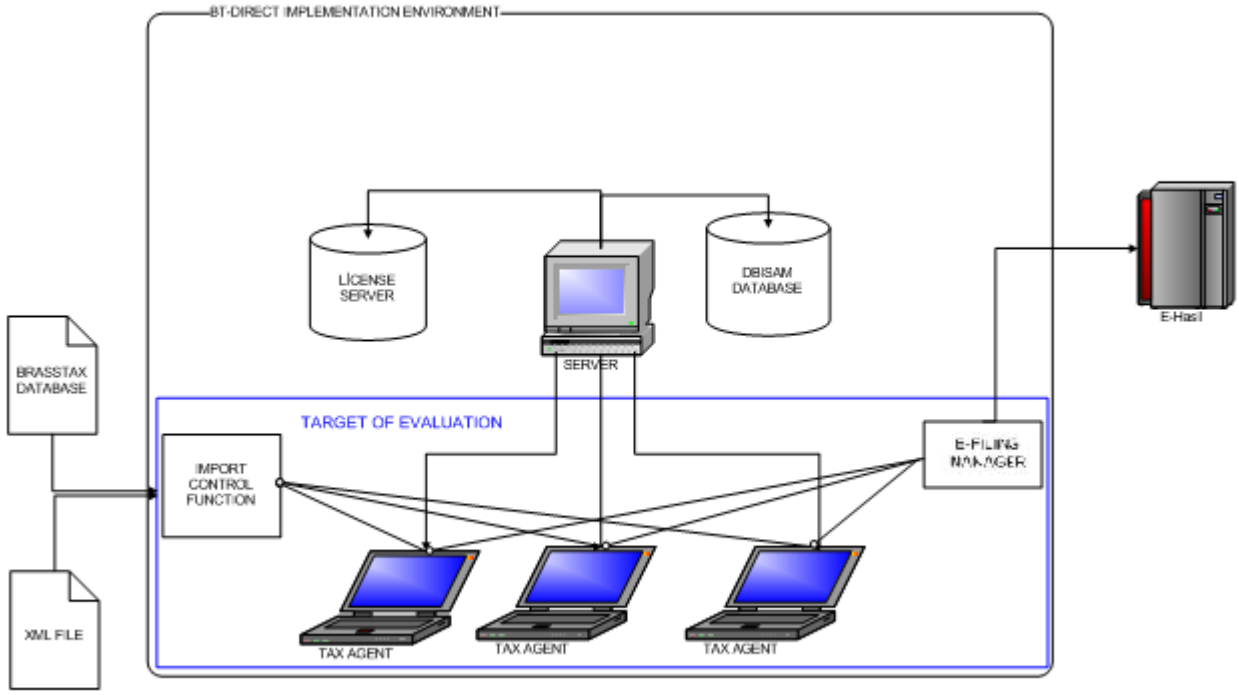

Figure 1 General BT-Direct System Architecture

The TOE is installed to the Tax Agent's computer in the above figure. Tax Agents are the users of the TOE.

BT-Direct System can be installed to any workstation with the following configuration;

- Processor: Pentium III (or above)
- RAM: 256 MB (or above)
- Hard disk space: 80 MB
- OS: XP (Home/Office), Vista, Windows 7
- Monitor: 800*600 (or better)
- IE v7 or higher
- Adobe Acrobat Reader 9 or higher

BT-Direct can be installed on a local area network where one of the workstations is designated as a server and the others are designated as clients. The designated server will host the license server and the Data Tables of the DBISAM Database. However DBISAM engine is embedded into the BT-Direct client workstations, and cannot be accessed by the user as a separate component.

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

The license server is a feature of the security wrapper and checked the validity of the license. This license server can be hosted in the designated server or any other workstations inside the network.

BT-Direct can also be installed onto a stand-alone PC. In this case the application, License Server will all reside on the same PC. It should be noted if this option is used, there is no option to allow data to be synchronized between other installations of BT-Direct (whether they be standalone or network installations).

After the installation of the BT-Direct Data files and License Server on the designated server machine, and following the installation of the Client Application on the workstations. The clients can start using the TOE only after launching the license server. Each client and their users can use the TOE according to their authorizations.

All the workstations which use BT-Direct can use their own e-Filing Manager during the communication with e-Hasil.

The communication with e-Hasil is provided by the LHDN infrastructure. The TOE version is currently using https connection, however the communication methodology is depending on the LHDN choice.

The Target of Evaluation is a subset of the BT-Direct System, where the Active X Controls, Security Wrapper, DBISAM Database and the communication interface with the e-Hasil are excluded, in addition to the Windows Operating System and Internet Explorer application which are accepted as the IT Environment. The scope and the boundaries of the Target of Evaluation and described in the latter sections.

Within the defined scope of the TOE, the TOE is the interface between the user and the e-Hasil system, where the users can perform all of the operations described above. In an other words the user interface and main functionalities of BT Direct and TOE is the same where some of the supporting features of the BT-Direct which were developed by third parties, like Active X Controls, Security Wrapper, DBISAM Database is accepted as IT Environment.

2.1 TOE Type

TOE is a software product with multiple user support in a local area network which mainly consists of the following five main modules and requires internet connection to the e-Hasil system;

- Import Module
- User Management Module
- Tax Agent Module
- Assessment Module
- e-Filing Manager

These modules are used with the security functions of the TOE and the communication functions with the IT Environment.

2.2 TOE Description

The TOE has physical and logical boundaries in its operational environment which consists of hardware and software components.

2.2.1 Physical Boundaries

TOE is installed to the workstations within a local area network and the hardwares 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, Active X Controls are not in the scope of TOE. These components are accepted as IT Environment which helps TOE to perform its intended operations.

The security wrapper which is accepted as an IT Environment component, provides two interfaces. These being a 'pass through' wrapper for the TOE, and remote IP Server, where access to the various modes is controlled using command-line parameters. As a pass through mechanism, the wrapper controls access to the TOE, by checking the validity of the license credentials which may be stored locally or remotely. As a Remote IP Server, the wrapper will store and provide security creditionals to interested clients applications operating using the 'pass through' wrapper. If the creditionals check out, then the wrapper will allow 'pass through' into the application software, otherwise the user will be blocked.

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

2.2.2 Logical Boundaries

The following figure is showing the logical boundaries and the modules of the TOE which differentiate it from its operational environment.

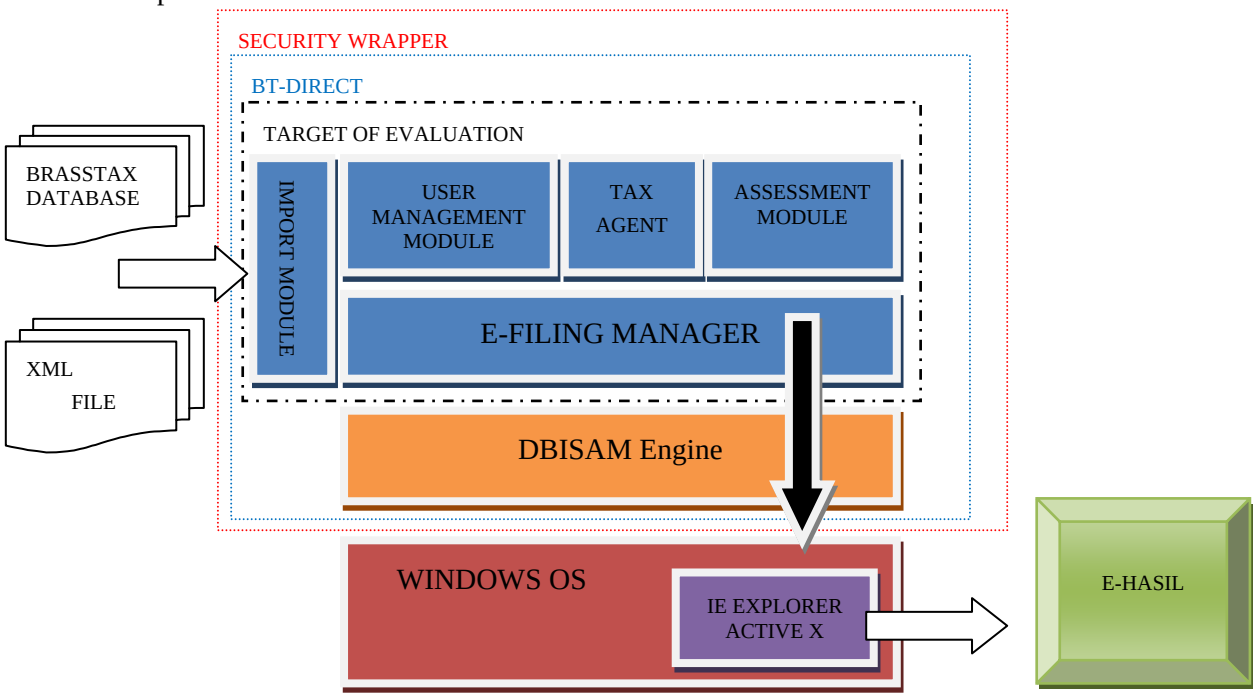

Figure 2 Logical Boundaries of the TOE

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.

User Management Module: This module allows the administrator to define and administer authorized users of the TOE, and allows authorized users to change their passwords. The functionality given to administrators allows them to also 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 relect the operation that was performed.

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 authorized users defined in the TAeF can have a user ID defined and can in turn be assigned to a given Assessment. The Tax Agent information defined in the TOE, should exactly match that which is defined in the TAeF. Each time the details in the Tax Agent module are changed, an entry will be made into the the Audit log.

Assessment Module: This module is used by authorized users for assessing the imported e-Borang data before sending to e-Hasil. The basic operations are create, update, delete and open assessment. It also allows user to look at their profiles and provides the necessary user interfaces to allow the authorized 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-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, these being:

• Register - This will attempt to 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 authorized user will be asked to confirm the assignment.

• Load - This will attempt to transfer all assessment information from the TOE into the TAeF.

• Draft - This will attempt to request the draft e-Borang from the TAeF for the current Assessment.

• 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.

• Sign - This will 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 authorized user may only request the final documents.

• Final - This function will attempt to 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.

2.3 TOE Security Features

TOE provides the following Security Features for secure operation;

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 5.

Data Protection: Access to the TOE features and data are subject to access control. Data Protection Function controls functions in Import Module and e-Filing Manager.

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.

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.

Addition to the above functions, the Operational Environment for the TOE provides time stamps for the audit logs.

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

3 SECURITY OBJECTIVES

This section defines the security objectives and the assumptions for the IT Environment of the TOE.

3.1 Security Objectives For The Operational Environment

The following security objectives must be satisfied by the user in order to use TOE in a secure manner.

Security Objective	Description
OE.INSTALL	The trusted users must install the TOE according to the preparative user guidance provided with the software.
OE.PHYSICAL	The users must ensure that the TOE is protected from physical attacks which might compromise the security objectives.
OE.USERS	Only the trusted and authorized users of the TOE must access to the TOE and ensure that they will only use the TOE in a secure manner according to the operational user guidance.
OE.SYNCTIME	The administrators of the TOE must ensure that the accurate server time is synchronized with the workstations in the operational environment.
OE.INTRUSION	The administrators of the TOE must ensure that the TOE is protected from external attacks from the network by an operational firewall.
OE.ANTIVIRUS	The administrators must ensure the security of the operational environment by installing and managing an antivirus software and a current virus definition file.
OE.BACKUP	The administrators must ensure that regular database back ups are taken and the back-ups are stored securely.
OE.IMPORT	The Users must ensure that files are imported to the TOE securely.

Table 1 Security Objectives for the Operational Environment

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

4 IT SECURITY REQUIREMENTS

This section specifies the requirements for the TOE addition to the operations that have been applied on the selected functional requirement components.

4.1 Extended Components Definition

4.1.1 Reliable Time Stamps

The following table contains the extended security functional requirements for the TOE:

Requirement Class	Requirement Components
FPT: Protection of TSF	FPT_STM_EXT.1 Reliable Time Stamps

FPT class contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF and to the integrity of TSF data. This component is a member of FPT_STM, an existing CC Part 2 family. The following extended requirement for the FPT class has been included in this ST because the operational environment is capable of providing reliable time stamps for TSF functions, which is not covered in CC Part 2.

FPT_STM_EXT.1 Reliable Time Stamps

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_STM_EXT.1.1 The operational environment shall be able to provide reliable time stamps for TSF functions.

Application Note: Reliable Time Stamps is required for the TOE to capture date and time events in relations to the FAU_GEN.1 and FMT_SAE.1 security functions. The TOE does not have feature to generate time stamps independently. However, the TOE is able to capture the date and time event from the environment which is derived from the Operating System.

4.2 TOE Security Functional Requirements (SFRs)

Requirement Class	Requirement Component	Dependencies
FAU: Security Audit	FAU_GEN.1	FPT_STM.1 Satisfied with FPT_STM_EXT.1
	FAU_GEN.2	FAU_GEN.1, FIA_UID.1
	FAU_SAR.1	FAU_GEN.1
	FAU_SAR.2	FAU_SAR.1
FDP: User Data Protection	FDP_ACC.1	FDP_ACF.1
	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
	FDP_DAU.1	No Dependency
	FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1
	FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1 FMT_MSA.3
FIA: Identification and Authentication	FIA_AFL.1	FIA_UAU.1
	FIA UAU.2	FIA_UID.1
	FIA_UID.2	No Dependency

FMT: Security Management	FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
	FMT_SMF.1	No Dependency
	FMT_SMR.1	FIA_UID.1
	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMF.1, FMT_SMR.1
	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1

Table 2 Security Functional Requirements

4.2.1 Security Audit (FAU)

4.2.1.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [**minimum**] level of audit; and

c) [**events listed in the table below**].

Audited Events	Related SFR	Description
Successful Log on	FIA_UID.2	The succesful authentication of a user
Log on Attempts	FIA_AFL.1	The authentication attempts of users
User Management	FMT_MSA.3,	Add, delete, update of a user
Security Group	FMT_SMR.1	Add, delete, update of a group
Assessment	FDP_ITC.1	An assessment is imported or deleted
e-Filing operations	FDP_ETC.2	Register, Load, Approve, Sign Assessment

Table 3 Audited Events

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].

4.2.1.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

4.2.1.3 Audit Review

FAU_SAR.1.1 The TSF shall provide [**administrator**] with the capability to read [**list of audited events**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

4.2.1.4 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.

4.2.2 User Data Protection

4.2.2.1 Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [**access control policy**] on [**authentication and the authorization of the users according to the associated security group**].

4.2.2.2 Security Attribute Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [**access control policy**] to objects based on the following:

[**List of Subjects;**

- **Administrator**
- **Tax Manager**
- **Staff**

List of Security Attributes;

- **Rights to show only assigned Borang**
- **Rights to delete assessment**
- **Rights to show assessment details**
- **Rights to change assessments**
- **Rights to import assessment**
- **Rights to file by batch**
- **Rights to register assessment**
- **Rights to upload assessment**
- **Rights to request draft**
- **Rights to approve**
- **Rights to request acknowledgment**
- **Rights to sign assessment**
- **Rights to maintain users**
- **Rights to maintain agents**
- **Rights to maintain default directories**
- **Rights to maintain security groups**
- **Rights to access reports**

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- **If the user is sucessfully authenticated according to his/her user group, then grant access according to the given rights.**
- **If the user attempt is unsuccessful then the requested access permission will be denied**
- **If the security group of the user have the right to access that subject.**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

4.2.2.3 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [**Submitted e-Borang to e-Hasil**].

FDP_DAU.1.2 The TSF shall provide [**Tax Manager, Staff**] with the ability to verify evidence of the validity of the indicated information.

4.2.2.4 Export of User Data With Security Attributes

FDP_ETC.2.1 The TSF shall enforce the [**access control policy**] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.2.2 The TSF shall export the user data with the user data's associated security attributes.

FDP_ETC.2.3 The TSF shall ensure that the security attributes, when exported outside the TOE, are unambiguously associated with the exported user data.

FDP_ETC.2.4 The TSF shall enforce the following rules when user data is exported from the TOE: [

Operation	Subject	Security Attribute	Rules
Export e-Borang to e-Hasil	**Staff**	**Tax Agent ID and Password** **Tax Payer ID and Password**	**XML Rules**

].

4.2.2.5 Import of User Data Without Security Attributes

FDP_ITC.1.1 The TSF shall enforce the [**access control policy**] when importing user data, controlled under the SFP, from outside of the TOE.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TOE.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TOE: [

Operation	Subject	Security Attribute	Rules
Import XML Files or Brasstax Data	**Staff**	**None**	**XML Rules**

].

4.2.3 Identification and Authentication

4.2.3.1 Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [**[3]**] unsuccessful authentication attempts occur related to [**user authentication during log on**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**met**], the TSF shall [**terminate the application**].

4.2.3.2 User Authentication Before Any Action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

4.2.3.3 User Identification Before Any Action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

4.2.4 Security Management

4.2.4.1 Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [**disable, enable**] the functions [**security group functions**] to [**administrator**].

Application Notes: New Users for TOE should be assigned to specific "security groups" which the security groups have specific access rights enabled or disabled by TOE administrators. The enabled security attributes (listed under 4.2.2.6) for a security group are assumed as "security group functions."

4.2.4.2 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- **Rights to maintain users,**
- **Rights to access reports,**
- **Rights to maintain security groups,**

].

Application Note: The following functions are accepted as management functions which can be performed by TSF;

Maintain Users: Add/Delete/Modify Users of TOE.

Access Reports: The permissions for accessing to audit logs.

Maintain Security Groups: Allow or Deny Security Attributes for security groups.

Authorised users can modify the above management functions through the TSF.

4.2.4.3 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [**administrator, tax manager, staff**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

4.2.4.4 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [**access control policy**] to restrict the ability to [**change_default, modify**] the security attributes [

- **Rights to show only assigned Borang**
- **Rights to delete assessment**
- **Rights to show assessment details**
- **Rights to change assessments**
- **Rights to import assessment**
- **Rights to file by batch**
- **Rights to register assessment**
- **Rights to upload assessment**
- **Rights to request draft**

- **Rights to approve**
- **Rights to request acknowledgment**
- **Rights to sign assessment**
- **Rights to maintain users**
- **Rights to maintain agents**
- **Rights to maintain default directories**
- **Rights to maintain security groups**
- **Rights to access reports**

] to [**administrator**].

4.2.4.5 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the [**access control policy**] to provide [**permissive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA 3.2 The TSF shall allow the [**administrator**] to specify alternative initial values to override the default values when an object or information is created.

4.3 TOE Assurance Requirements (SARs)

Requirement Class	Requirement Component
ADV: Development Class	ADV_FSP.1 Basic Functional Specification
AGD: Guidance Documents	AGD_OPE.1 Operational User Guidance
	AGD_PRE.1 Preparative User Guidance
ALC: Life Cycle Support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM Coverage
ATE: Tests	ATE_IND.1 Independent Tests
AVA: Vulnerability Assessment	AVA_VAN.1 Vulnerability Survey
ASE: Security Target Evaluation	ASE_CCL.1 Conformance Claims ASE_ECD.1 Extended Components Definition ASE_INT.1 ST Introduction ASE_OBJ.1 Security Objectives for the Operational Environment ASE_REQ.1 Stated Security Requirements ASE_TSS.1 TOE Summary Specification

Table 4 Security Assurance Requirements

5 TOE SUMMARY SPECIFICATIONS

5.1 TOE Security Functions

5.1.1 Audit Function

This functionality is implemented in order to meet the following requirements;

- FAU_GEN.1,

- FAU_GEN.2,
- FAU_SAR.1,
- FAU_SAR.2

The audit function of the TOE is implemented for generating audit data logs for the defined events and the selected reviews of the generated audit logs.

An audit log will be created in the database when one of the following events will occur;

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.

Table 5 Auditable Event Details

In case of the realizations of the defined set of events, TOE will generate and audit log which only the authorized administrator can be able to review.

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 dependency for reliable time stamps are met with the extended component FPT_STM_EXT.1. The TOE receieves the time stamps from the operating system and record time for the audited events.

5.1.2 User Data Protection Function

This functionality is implemented in order to meet the following requirements;

- FDP_ACC.1,
- FDP_ACF.1,
- FDP_DAU.1
- FDP_ETC.2,
- FDP_ITC.1

User Data Protection Functionality is providing the capability to the TOE for implementing an access control for the authorized users according to 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 authorizations of the users and deny the access requests to the objects that is not allowed.

The import of user data is controlled by access control policy and checks the access rights of the subjects before a request to access an object.

The export of the Tax Profile to the e-Hasil is managed by the communication interface with e-Hasil. The XML Rules used to define the define the steps that will be used to export the data. Export of user data is associated with the security attributes of the user (User ID, Password).

A basic data authentication functionality is performed by the TOE by generating evidence for unsuccessful uploads to the e-Hasil. An error message is provided to the user if the user data is not uploaded to the correct place or the upload process is failed for any reason. The user could restart the process upon the unsuccessful upload operation.

5.1.3 Identification and Authentication Function

This functionality is implemented in order to meet the following requirements;

- FIA_AFL.1,
- FIA_UAU.2,
- FIA_UID.2

This functionality is covering the authentication failures, user authentication and identification before any action.

Authentication failures is counting the number of unsuccessful attempts, and when the defined value (3) have 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.

The users must be properly authenticated and identified in order to conduct any operations within the TOE.

5.1.4 Security Management Function

This functionality is implemented in order to meet the following requirements;

- FMT_MOF.1,
- FMT_SMR.1,
- FMT_SMF.1,
- FMT_MSA.1,
- FMT_MSA.3

Security Management Functions are providing the management of security functions and security roles. This functionality is provided mainly by creating security groups by the administrator. The administrators can be enable or disable the functionalities for the specified user group where the TSF enforce the authorized functionalities. These security groups and users associated with the groups are managed by the TSF.

Access Control according to the defined user groups and identified User ID handled by the TSF.

Management of Security Attributes of users and/or user groups can only be conducted by authorized users. Within the scope of recommended configuration only TOE administrators can modify these values where tax manager and staff roles can not be able to change or modify those attributes. After the proper installation of the TOE according to the guidance documents the TSF will restrict this functionality to administrator.

The list of security attributes for user groups are permissive by default and the values for these attributes can be changed by administrators within the scope of static attribute initialization.

APPENDIX A ACRONYM LIST

CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ST	Security Target
SFR	Security Functional Requirements
TOE	Target of Evaluation
TSF	TOE Security Functions
IT	Information Technology
SFP	Security Function Policy
TSF	TOE Security Functions
TSP	TOE Security Policy

Table 6 Acronyms List

The contents of this document are the property of EA Link System SDN BHD and should not be reproduced, copied or disclosed to a third party without the written consent of the proprietor.