EA LINK SYSTEM SDN BHD

TAXSAYA

COMMON CRITERIA

EAL1 CERTIFICATION

TAXSAYA ONLINE Version 1.5.0.12

SECURITY TARGET

Version No	1.1		
Revision Date	07/02/2013		
Document Code	TOV-ST-11		
File Name	TOV-ST-1.1.DOC	**Language**	ENGLISH
Project	TAXSAYA ONLINE VERSION COMMON CRITERIA EAL1 EVALUATION PROJECT		
Title	TAXSAYA ONLINE Version 1.5.0.12 SECURITY TARGET		
Category	DELIVERABLE		
Prepared By	FIRMUS SECURITY SDN BHD		

Version History

Version No	Reason for Change	Release Date
0.1	First Release	25/02/2011
0.2	Update According to the comments from Vendor	10/03/2011
0.3	Update According to the changes in TOE	10/06/2011
0.4	Change in the scope of TOE	19/10/2011
0.5	Consistency check according to the comment from Stratsec	25/10/2011
0.6	Update according to the EOR001 from the Evaluation Facility	27/12/2011
0.7	Update according to the EOR001 v2.0 from the Evaluation Facility	05/01/2012
0.8	Update according to the Progress Meeting Minute #2	28/02/2012
0.9	Update according to the EOR001 v3.0 from the Evaluation Facility	02/05/2012
1.0	Update according to the Observation Report Responses	28/01/2013
1.1	FIA_SOS requirement is updated in accordance with the Identification Authentication Function	07/02/2013

Approvals

Name	Role	Date
Mehmet ÇAKIR	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

Comments

CONTENT

INDEX OF TABLES

INDEX OF FIGURES

Version No: 1.1	Rev. Date: 07/02/2013	TOV-ST-1.1	6.th page of	18 pages

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	: TAXSAYA Online Version 1.5.0.12 SECURITY TARGET
ST Version	: 1.1
ST Authors	: Mehmet Çakır (Firmus Security), Trevor Keegan (EA Link)
Date of Publication	: 07/02/2013
TOE Software Identification	: TAXSAYA Online Version 1.5.0.12
Developed By	: EA Link System Sdn. Bhd.
Evaluation Assurance Level	: EAL 1
Keywords	: Tax, e-Borang, e-Filing, IRB, e-Hasil, LHDN, Malaysia, MyCC,

MyCB, MySEF, Common Criteria, Common Evaluation Methodology, Evaluation Assurance Level, Information Security.

1.2   CC Conformance Claim

This ST is consistent with the following specifications:

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

The TOE is consistent with the claims defined in this ST and conformant to EAL1 according to Common Criteria Version 3.1 Revision 3.

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 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 security policy of the TOE which controls access from controlled subjects.

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

EA Link Administrator: Users which maintain TOE through Microsoft Azure interface provided by Microsoft.

1.3.3 Acronyms

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

2   TOE OVERVIEW

TOE is a web application which is hosted by Microsoft Azure servers and the application can be used by the customers as a service through the internet. Main functionality of the TOE is to assist Taxpayers to prepare and submit their Tax Returns.

Users of the TOE can access their accounts via Internet Explorer or Firefox. After a successful authentication process the users are prompted to provide necessary information in order to prepare their tax returns. TOE provide an interview style tax wizard to support users to fill all the required fields to complete the operation. A tax optimizer provides the Taxpayers with suggested tax savings, and the final tax file can either be printed or automatically filed with the Tax Department.

The software can be used in any computer with an internet access and a browser where the accounting is handled with the user name and password which is used as a unique identifier for each user. The taxpayer is simply prompted to fill in the necessary inputs in order to calculate the possible tax refund. The information provided by the user is stored in a database and upon request by the user the information can be transmitted to the e-Hasil system with an automatic logon support. The users can also generate reports anytime for further audits.

The following operations can be performed with TAXSAYA user interface;

- Identification and Authentication,
- Calculation of Tax Returns electronically,
- Re-use of data derived from previous year,
- Produce paper based Borang,
- Produce reports for tax audit,
- Tax optimization

TaxSaya Online provides the following features to the authenticated users;

- **User Interface Module:** This module is providing the identification and authentication of the client 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 not correct 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.
- **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 enter in the password. The TOE will then transfer all Assessment information into the e-Filing, and attempt to download the Draft e-Borang.
- **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.
- **Reporting Module:** This module allows the user to print a template of the final borang. In addition, the user can request the system to prepare a detailed report that itemizes all the income

and expense details that have been entered, to show how the figures in the Borang have been computed.

Administrative functions of the TOE is handled by EA Link administrators through their acounts on Microsoft Azure Platform. The EA Link Administrators conducts the following actions which are outside the scope of TOE and its CC evaluation;

- Maintenance of user acounts,
- Maintenance of software,
- Audit Review,
- Back-ups
- Allocating/deallocating additional system resources

2.1 TOE Type

TAXSAYA is an web application which the users access with their own user name and password from the Microsoft Azure servers dedicated to EA Link via an Internet Explorer or Firefox. The scope of the CC evaluation is including the software service provided by the vendor through an application server and the interface between the users of the TOE.

The Minimum System Requirements for the users of the TOE are;

- Windows XP
- IE v7 or Firefox v3
- Adobe Acrobat Reader 9
- Any workstation configuration compatible with the above applications,

The System Requirements for the TOE application are;

- Microsoft Azure Server configured with IIS, Azure SQL and .NET v4.0

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 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.

TOE is running on an application server and the users can access to the functions of the TOE upon successful authentication through the web adress. Users can perform operations through a web browser however the web browser that users use are outside the physical scope of the TOE.

The platform that runs the TOE is a cloud service which is hosted by Microsoft. Upon the installation of TOE to the EA Link acount, TOE starts to provide its services to the users through internet.

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.
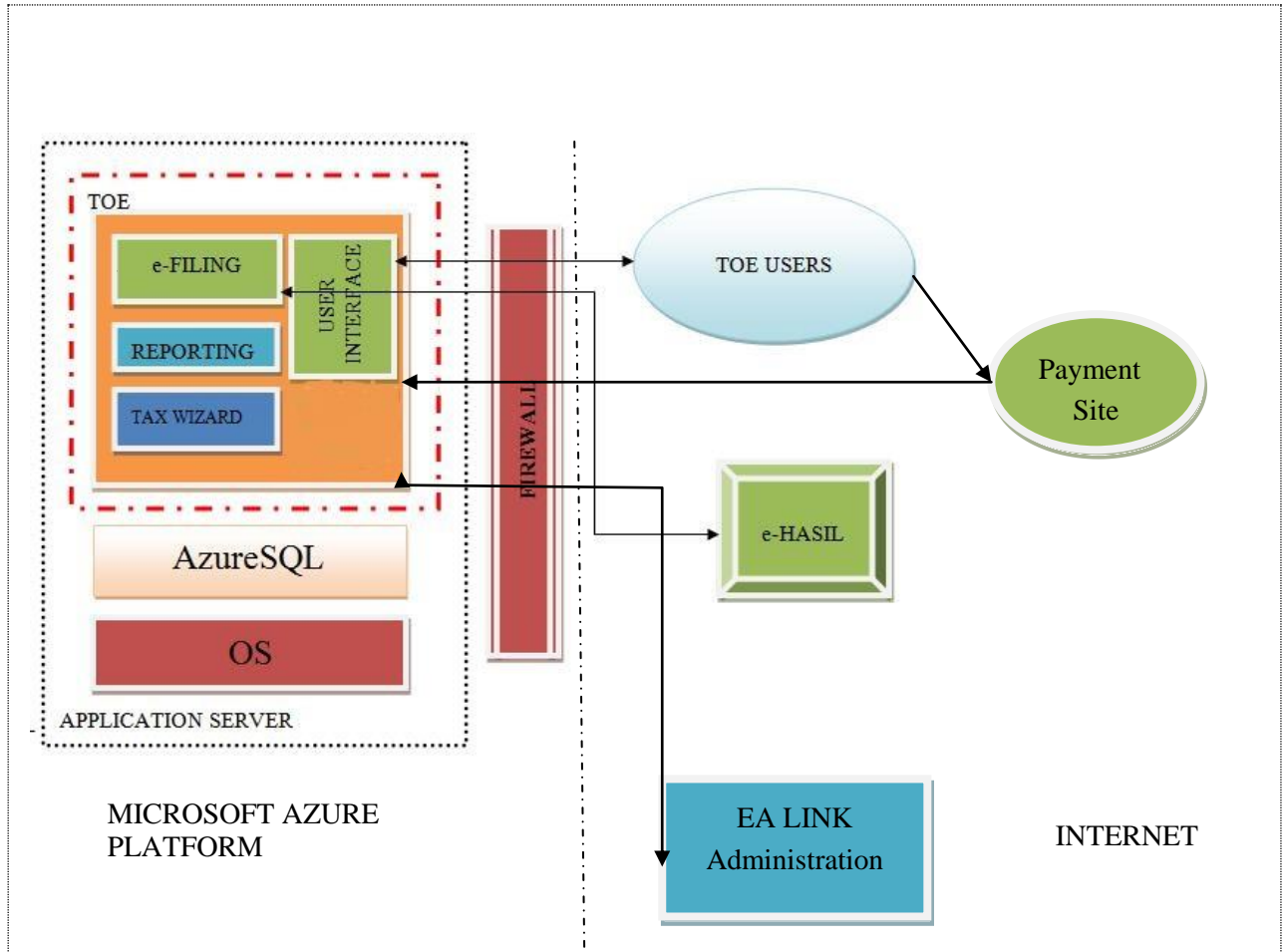
Figure 1 Logical Boundaries of the TOE

TOE is providing its service in the cloud system provided by Microsoft Azure Platform. EA Link created its acount from the hosting site which includes a virtual machine for the application and a SQL server.

TOE is only used by authenticated TOE Users through the website www.taxsaya.com. Upon completing registration the users directed to a payment site hosted by iPay88. When the user complete the payment for creating the acount, payment site sent an activation link to TOE. TOE then change the status of acount which is created during registration on the SQL Server. After completion of the registration process the user is directed to the site www.taxsaya.net for using TaxSaya Online version hosted in Microsoft Platform.

TOE provides the following security functions;

- **Audit Logs:** TOE generates audit logs for the auditable events listed in section 5.1.1. 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.

- **Identification and Authentication:** TOE identify and authenticate its users before any action. All registered users have a User Name and Password in order to complete the identification and authentication process.

- **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.

- **Management of Security Attributes:** TOE support the management of security attributes belong to the users.

Administrative functions of TaxSaya including database management and maintenance of the software is conducted through an acount provided by Microsoft Azure. These functionalities are outside the scope of evaluation.

Version No: 1.1	Rev. Date: 07/02/2013	TOV-ST-1.1	10.th page of	18 pages

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.USERS	The administrators of the EA Link must install and manage the TOE in a secure manner.
OE.PHYSICAL	The TOE must be installed in a physically secure area.
OE.HARDENED	The Microsoft Azure Platform must ensure the host system is hardened. For example, it's protected from external attacks from the network by an operational up to date firewall; installed with an antivirus software and a current virus definition file; secured with password etc.
OE.BACKUP	The administrators of the EA Link must ensure that regular database back ups are performed and the back-ups are stored securely.
OE.SECCOMCHANNEL	Communication between users and TOE are passed through an encrypted secure channel via SSL connection to the TOE.

Table 1 Security Objectives for the Operational Environment

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

All the requirements stated in this Security Target have been selected from the Common Criteria Version 3.1 Revision 3. So there are no extended components definitions to be declared.

4.2   TOE Security Functional Requirements (SFRs)

Requirement Class	Requirement Component	Dependencies
FAU: Security Audit	FAU_GEN.1	FPT_STM.1
	FAU_GEN.2	FAU_GEN.1, FIA_UID.1
FDP: User Data Protection	FDP_ACC.1	FDP_ACF.1
	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
	FDP_ETC.2	FDP_ACC.1 or FDP_IFC.1
FIA: Identification and Authentication	FIA_AFL.1	FIA_UAU.1
	FIA_ATD.1	No dependencies
	FIA_SOS.1	No dependencies
	FIA_UAU.2	FIA_UID.1
	FIA_UID.2	No dependencies
FMT: Security Management	FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMR.1, FMT_SMF.1
	FMT_MSA.3	FMT_MSA.1, FMT_SMR.1
	FMT_SMF.1	No dependencies
	FMT_SMR.1	FIA_UID.1

Table 2 Security Functional Requirements

4.2.1   Security Audit

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 [**basic**] level of audit; and

   c) [**none**].

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**].

Application Note: The dependency for the functional requirement FPT_STM.1 is not met in the TOE since the reliable time stamps is not provided by the TOE but the TOE take the date/time information from the operational environment.

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.

4.2.2   User Data Protection

4.2.2.1   Subset Access Control

FDP_ACC.1.1 The TSF shall enforce the [**data export access control policy**] on [

List of Subjects;

Authorised Users

List of Objects;

Tax Data

Operations;

Upload Objects to e-Hasil

].

4.2.2.2   Security Attribute Based Access Control

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

List of Objects;

Authorised Users

List of Subjects;

Tax Data

Security Attributes;

User Name

Password

IC Number

].

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

IC Number and e-Hasil Password of the user is correct at the e-Hasil site

].

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   Export of User Data With Security Attributes

FDP_ETC.2.1 The TSF shall enforce the [**data export 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: [**none**].

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 [**lock user account**].

4.2.3.2 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**username, password, IC Number**].

4.2.3.3 Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**min 6-max 16 characters, check for three out of four requirements lower, upper case, numbers and symbols**].

4.2.3.4 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.

4.2.3.5 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 Attributes

FMT_MSA.1.1 The TSF shall 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**].

4.2.4.2 Static Attribute Initialisation

FMT_MSA.3.1 The TSF shall enforce the [**data export 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 [**users**] to specify alternative initial values to override the default values when an object or information is created.

4.2.4.3 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**change user password**].

4.2.4.4 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles [**users**].

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

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 Procedures
ALC: Life Cycle Support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM Coverage
ATE: Tests	ATE_IND.1 Independent Testing-conformances
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 3 Security Assurance Requirements

5   TOE SUMMARY SPECIFICATIONS

5.1   TOE Security Functions

5.1.1   Audit Logs

Reporting Module is generating audit logs for the list of audited events in the table below. Audit logs are written to the Microsoft SQL database with the attachment of data/time information taken from an NTP server. Each audit log is including date and time of the event, type of the event, subject identity and outcome of the event.

Requirement	Description
FAU_GEN.1	Start up and shutdown of the audit function.
FDP_ACF.1	All data export requests from users to e-Hasil
FDP_ETC.2	All attempts to export information
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts.
FIA_SOS.1	Rejection of acceptance of any tested secrets.
FIA_UAU.2	All use of authentication mechanism.
FIA_UID.2	All use of identification mechanism.
FMT_MSA.1	All modifications to the security attributes.
FMT_MSA.3	Modifications to the initial values.
FMT_SMF.1	Use of management functions.
FMT_SMR.1	Managing the group of users.

Table 4 List of Audited Events

Audit logs are generated by the TOE with the association of the user and the event. All the auditable events are logged with a user who performs the operation within the TOE.

The following functional requirements are covered by this security function;

FAU_GEN.1, FAU_GEN.2

5.1.2   Identification and Authentication

User Interface Module is enforcing an identification and authentication mechanism before any actions on TOE. Users can generate their own user name and passwords according to a defined metric enforced which checks the password if it contains at least three of the following four requirements ;

   a.   Lower Case Characters,
   b.   Upper Case Characters,
   c.   Numbers,
   d.   Symbols,

Identification and Authentication function also allows users to select passwords up to 16 characters which must be at least 6 characters. Users can request a new password if they forgot the previous one and after a confirmation process users can generate their new passwords.

TOE also maintain IC Number as well as the username and password for each user for authentication to the E-Hasil site during data export.

Authentication attempts are counted by TSF and if the number of unsuccessfull authentication attempt is reached to 3, the associated user acount will be locked for 24 hours.

The following functional requirements are covered by this security function;

FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2.

5.1.3   Tax Data Export

Users can upload their tax data to the e-Hasil by using the e-Filing module of the TOE. TSF 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.

The following functional requirements are covered by this security function;

FDP_ACC.1, FDP_ACF.1, FDP_ETC.2

5.1.4   Management of Security Attributes

Management interface allow users to manage security functions of the TSF and also to manage the security roles within the TOE. Tthe TSF also automatically allow/deny access attempts, enforce access control policy, manage user sessions.

Following security attributes for each users are managed by TSF;

    a.   Username
    b.   Password
    c.   IC Number

The following functional requirements are covered by this security function;

FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1

© 2013 EA Link System SDN BHD
B2-05, Block B, 2nd Floor, SME Technopreneur Centre
2270 Jalan Usahawan 2, 63000 Cyberjaya Selangor
Phone: +603 8315 6020 Fax: +603 8315 6021

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 5 List of Acronyms