C021 Certification Report

ePassport Suite v2.5

File name: ISCB-5-RPT-C021-CR-v1a

Version: v1a

Date of document: 8 July 2011

Document classification: PUBLIC

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

C021 Certification Report
ePassport Suite v2.5

8 July 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:	C021 Certification Report – ePassport Suite v2.5
DOCUMENT REFERENCE:	ISCB-5-RPT-C021-CR-v1a
ISSUE:	v1a
DATE:	8 July 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 8 July 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	30 June 2011	All	Final Released.
v1a	8 July 2011	Page iv	Add the date of the certificate.

Executive Summary

The ePassport Suite v2.5 (hereafter referred as ePassport Suite) from Extol MSC Berhad is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

ePassport Suite is an authentication system which provides Two-Factor Authentication (2FA) by requiring users to key in username, and One-Time-Password (OTP) from these tokens; ePassport Suite Hardware generator, ePassport Suite software desktops or ePassport Suite application in mobile phone. If the authentication process is successful, users will be allowed to access the intranet web applications.

ePassport Suite comprises of the following:

- Core Engine of ePassport Suite - is the main component that enforces the cryptographic functionality of the two-way authentication functions.
- Management Console is the interface for administrator to manage the users and ePassport Suite system.
- Platform for systems integration with ePassport Suite via Radius, Web services, JDBC and LDAP. However, this is not in the scope of the evaluation.
- Applications, certifications and tokens use with ePassport Suite in its operations that suite the client requirement.

The modules of the ePassport Suite that are within the scope of the evaluation include all modules in Management Console, Authentication and Cryptography modules of the Core Engine, and Mobile and Desktop tokens.

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

This report confirms the findings of the security evaluation of ePassport Suite to the Common Criteria (CC) evaluation assurance level EAL1. The report confirms that the product has met the target assurance level of EAL1 and the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by CyberSecurity Malaysia Security Evaluation Facilities (MySEF) and the final Evaluation Technical Report (ETR) received on 30 June 2011.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the ePassport Suite evaluation meets all the conditions of the MyCC Scheme requirements 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 ePassport Suite meets their requirements. It is recommended that a potential user of the ePassport Suite to refer to

the Security Target (Ref [6]) and 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), ePassport Suite v2.5, is a web based authentication system which supports a suite of authentication mechanisms to secure user accounts, intranet web apps and online transactions.

2 The ePassport Suite v2.5, which is installed behind an internet gateway firewall, is providing a secure remote access with security implementation of Two-factor Authentication (2FA) for the users. The users of the ePassport Suite could integrate any application which require authentication. Any system that is able to seek authentications via web service protocol or radius will be able to utilize the facility.

3 The ePassport Suite v2.5 requires users to provide two means of authentication by enforcing usage of username, and One-Time-Password (OTP) replacing the normal password mechanism. OTP generated by application pre-installed inside several mobility platform such as mobile phone (java application), hardware token and desktop (software application).

4 ePassport Suite v2.5 comprises of four major components as follows:

a) Core Engine;

b) Management Console;

c) Type of Systems Integrated with ePassport; and

d) ePassport Suite type of Applications, Certifications and Tokens.

The details of these major components will be described further in Section 1.4 of this report.

5 The security functions of ePassport Suite v2.5 which had been evaluated are:

a) Audit – logs are captured if there are system wide changes (overall changes happening on the ePassport Suite), authentication attempts and system status. This function provides the capability to generate system reports, TOE system logs for accounting performed by users.

b) Authentication – based on the user credentials. Authentication process is performed by Authentication module of Core Engine, and supported by ePassport Suite Tokens specifically desktop software and mobile phone application that generates OTP.

c) Cryptography – performed by Cryptography module of Core Engine, and ePassport Suite Tokens specifically desktop software and mobile phone application.

d) Security Management – User, Token and Server management of the ePassport Suite are configured by the Administrators via the Management Console.

1.2 TOE Identification

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

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C021
TOE Name	ePassport Suite v2.5
TOE Version	v2.5
Security Target Title	Extol ePassport Suite v2.5 Security Target
Security Target Version	v2.0
Security Target Date	30 June 2011
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 Extended CC Part 3 Conformant Package conformant to EAL1
Sponsor and Developer	Extol MSC Berhad Unit G1, Ground Floor, Wisma UOA Pantai,No. 11, Jalan Pantai Jaya, 59200 Kuala Lumpur, Malaysia
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

7 Access control policy inside the TOE is applied to the users according to the system groups that they belong to and their rights to access the subjects within the TOE. When the users key-in their user ID and password, TOE confirms the access rights of the users according to its group memberships.

8 The TOE implements password policy where the length, complexity and maximum attempt of the password can be configured by the Administrator.

9 The TOE implements information flow control policy to manage the flow of the information by allowing or restricting access to a specific list of objects and conduct a defined list of events. Administrators have the right to modify the policy.

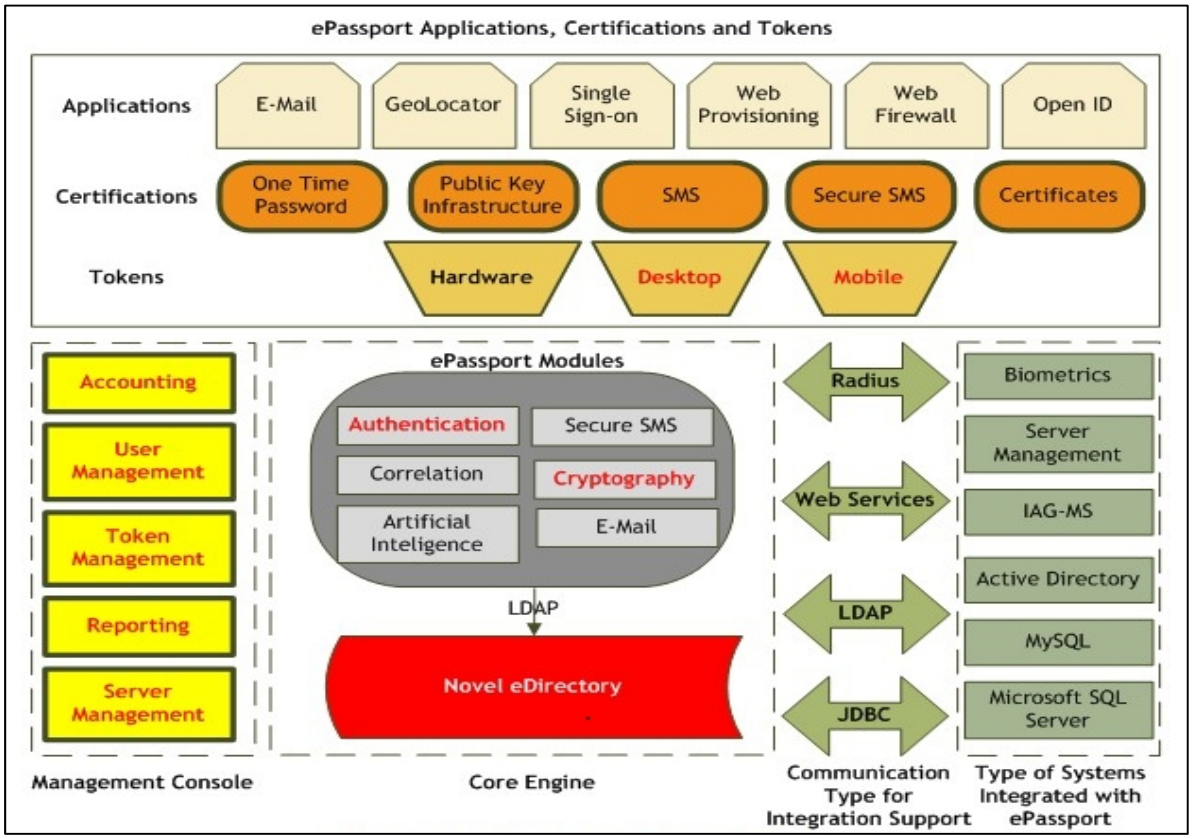
10 Details of the security policies are described in Section 4 and Section 5 of the Security Target (Ref [6]).

1.4 TOE Architecture

11 The TOE includes both logical and physical boundaries which are described in Section 1.4 of the Security Target (Ref [6]).

12 The following

13 Figure 1 describes in detail the logical scope of the ePassport Suite v2.5 that



comprises the TOE. The words in RED font and bold is the scope of TOE.

Figure 1: TOE Logical Scope

14 ePassport Suite v2.5 comprises of four major components in its architecture as follows:

a) **Core engine** – consist of the ePassport Suite Modules where Authentication and Cryptography Modules are in the scope of the evaluation. The rest of the modules Secure SMS, Correlation, Artificial Intelligence, and E-Mail shown in the Figure 1 are optional modules which can be integrated to the TOE. The Novell eDirectory is used via the LDAP and is a part of the IT environment. Core Engine performed most of the major functionalities of ePassport Suite in aspects of handling the information related to TOE operation and data.

b) **Management Console** – interface where the system can be configured by the Administrators. The Management Console consists of the Accounting, User Management, Token Management, Reporting and Server Management modules.

c) **Systems Integrated with ePassport Suite** – The Authentication in ePassport Suite modules is able to integrate with other applications that the TOE supports based on services of Authentication. The TOE provides integration via Radius, Web Services, JDBC and LDAP.

d) **ePassport Suite type of Applications, Certifications and Tokens** – List of applications, certifications and tokens that can be used with ePassport Suite in its operations. Applications are a system has been implemented in the client side that required ePassport Suite in providing security enforcement. Certifications are also part of the implementation in the IT environment. Tokens are devices or software that providing data in aspects of random numbers, enforcing the requirement of Two-Factor Authentication process (2FA).

Note: Refer to Figure 1 for illustration details.

15 The Core Engine and Management Console of the TOE are installed to a designated server within a local area network. The TOE can be accessible by the users via web services with the workstation inside or outside of the network. However, Administrators are allowed to access the TOE only from the intranet network.

16 The services provided by ePassport Suite v2.5 to the desktop and mobile users are configured and maintained by two types of users as follows:

a) Administrators – who has all the administrative rights in the Management Console.

b) System Users – created by the Administrators. System Users will be assigned to specific system groups and appropriate access rights will be given where specific and limited privileges to access, limited viewable access and limited rights in operating the TOE. System Users, who are accommodating with tokens, are known as Token Users.

1.5 Clarification of Scope

17 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]). Each security functionalities can then be divided to several sub-component and includes only the following evaluated security functionality:

a) **Audit** – provides the capability to generate system reports, TOE system logs for accounting performed by users. It also provides the scope of the reporting functionality.

i) **Accounting (Management Console) –** captures logs for all system changes happening on the ePassport Suite, authentication attempts and system status. Logs captured are stored in the Postgres database provided by Novell's eDirectory system in the Core Engine and the access to the database is password protected.

ii) **Reporting (Management Console) –** provides means of presenting logs information from the Postgres database. Reporting presents the logs in

graphical information that easily capture by Administrators and exports in printable formats.

b) **Authentication** – provides the means to check the user's credential and the authentication process with supported by Tokens to identify user's access right to the TOE.

   i) **Authentication Module (Core Engine) –** provides interface for administrator to configure administrative for token users. Administrator will have access to the Authentication Module setting via web browser in the Management Console. User's credentials are stored at the Novell's eDirectory together with user's access right, policy, and other related information. Authentication process is divided into two separated methods authentication of username and password; and checking of token users credential. Authentication of token is done at the ePassport Suite server and checks with its internal algorithm for verification.

   ii) **Tokens (ePassport Suite Tokens) –** users key in their OTP at the login page, and the TOE then sends an OTP sequence number through SOAP. The SOAP communication then sends the OTP to authentication module for verification. Pass or fail verification is then sends back to the login page via SOAP. There are two types of token declared in the scope of evaluation and that is Desktop Software Token and Mobile Phone Token.

c) **Cryptography** – is used in ePassport Suite application for mobile phones token, ePassport desktop software token, and ePassport Suite licensing function.

   i) **Cryptography Module (Core Engine)** – performs cryptographic functions for token registration and OTP generation in mobile and desktop token. In ePassport Suite server, cryptography module is used to encrypt the licensing file from unauthorized editing. Token generated from the mobile and desktop application are not linked to the ePassport Suite servers in terms of token generation. Each token are randomly generated individually at the mobile and desktop. The ePassport Suite server have its own algorithmic mechanism to verify the randomly generated tokens.

   ii) **Token (ePassport Suite Tokens) –** tokens are created during registration of the user to the ePassport. Tokens are generated from input from a sequence of number is provided by the ePassport Suite server. This input together with the user ID will be an input to the OTP Generator. Details of the token generation are explained further in section 5.1.3 of the Security Target (Refer [6]).

d) **Security Management –** there are three type of security management within the scope of ePassport Suite v2.5 evaluation; user management, token management and server management. It functions as a centralised management accessibility of the TOE for the administrator to perform maintenance, setting, and configuration of any related functions for operation of the TOE.

   i) **User Management module (Management Console) –** provides means for the administrator to manage user access to intranet resources functionality of the TOE. Administrator can also customise privilege access to user for access to the management console for viewing purpose. In the User

Management module administrator are given functionality to manage user policy, add, modify and delete users and their privilege. Group, user roles management and session each user as individual and as a group can also be defined. User's information are stored in Novell eDirectory however access rights are defined in LDAP.

ii) **Token Management (Management Console)** – provides administrator functionality to manage (add, modify and delete) token users. Administrator can also add or assign authentication function (mobile token or desktop token) for each token user. Token user's information is stored in the Novell eDirectory. Request to view the information are extracted from Novell eDirectory via LDAP.

iii) **Server Management (Management Console)** – provides ability to manage multiple ePassport Suite authentication server with a single console. ePassport Suite server can be established and setup in a multiple appliance within either in a single network or in different network.

18 It is important to note that the TOE can support other services that are also provided by the developer of ePassport Suite v2.5. However, these functions and services are not evaluated. Potential consumers should carefully consider their requirements if they intend to use these functions and services as it is outside of the evaluated configuration.

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

a) Hardware token;

b) Secure SMS module;

c) Correlation module;

d) Artificial Intelligence module;

e) E-mail module;

f) Novel eDirectory through LDAP;

g) Other ePassport application, certificates and Tokens;

i) E-mail

ii) GoeLocator

iii) Single Sign-on

iv) Web Provisioning

v) Web Firewall

vi) Open ID

vii) Public Key Infrastructure

viii) SMS

ix) Secure SMS; and

x) Certificates

1.6 Assumptions

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

1.7 Evaluated Configuration

21 ePassport Suite v2.5 can be distributed by the developer in form of appliance or software based. However, for this security evaluation, the TOE is delivered in software based.

22 The TOE is configured according to the Installation Guide (Ref [10]). The developer will install the required environment in sequence as follows:

a) Novell 10.2 installation guide

b) Postgresql installation

c) Novell eDirectory installation

d) Generate ePassport Environment

e) Tomcat 6 installation

f) Finalized Steps

1.8 Delivery Procedures

23 ePassport Suite v2.5 is delivered, installed, and configured to the user by the developer's authorised personnel.

24 For this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, developer did not provide any documentation on TOE delivery and the evaluators did not verify any TOE delivery process. In security objectives of the operational environment in Security Target (Ref [6]), OE.INSTALL stated that the person responsible of TOE must ensure that the TOE and any hardware/software required by the TOE are delivered, installed, and managed by a responsible authorized personnel. Therefore, the evaluators relied on the environment to provide a secure TOE delivery process.

1.9 Documentation

25 It is important the ePassport Suite v2.5 is used in accordance with guidance documentation in order to ensure secure usage of the product.

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

a) ePassport Suite Administrative Guide EC-5750-eP1000 (Standard Edition) (Refer [9]).

b) ePassport Suite User Guide EC-5750-eP1000 (Standard Edition) (Refer [8]).

27 The following guidance documentation is provided by the developer for secure installation and usage of the product:

a) EXTOL ePassport Suite v2.5 Security Target (Refer [6]).

b) ePassport Installation Guide (Refer [10]).

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 ePassport Suite v2.5, including the following components:

2.1.1 Life-cycle support

30 An analysis of the ePassport Suite v2.5 configuration management system and associated documentation was performed. The evaluators found that the ePassport Suite v2.5 configuration items were clearly and uniquely labelled, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items.

2.1.2 Development

31 The evaluators analysed the ePassport Suite v2.5 functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

2.1.3 Guidance documents

32 The evaluators examined the ePassport Suite v2.5 installation guide and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

33 Testing at EAL1 consists of assessing performing independent function test, and performing penetration tests. The ePassport Suite v2.5 testing was conducted at CyberSecurity Malaysia MySEF 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 the evaluation conducted by evaluator based on the information gathered by examining functional and guidance documentation, and creating test cases to verify the behaviour of the TOE.

35 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Independent functional tests were developed and performed by the evaluators to verify the TOE functionality are as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
This test group comprises a series of test cases on TOE security functions of audit records generation and review for relevant authentication and management events bound towards the timestamp provided by the underlying operating system, such as: a) Failed authentication attempt b) Success log on c) Adding a user d) Adding a group e) Deleting a user f) Time-out session	Audit (Accounting + Reporting)	• Accounting <-> Novel eDirectory • User <-> Reporting • Accounting <-> User Management • Accounting <-> Token Management • User<-> User Management • Accounting <-> Authentication	Pass
This test group comprises a series of test cases on TOE security functions to verify unique identification & authentication by password/ OTP with access rights assigned to an individual user or a user groups within TOE.	Authentication	• User <-> Authentication • User<-> User Management • User Management<-> Authentication	Pass

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
This test group comprises of test cases on TOE security functions for the administrator to configure and manage the TOE and TOE system users (either as in individual or as groups). The test will cover: a) User and role management. b) TOE security management such as sessions and monitoring of accessibility. c) Access control rights. d) Default values, settings and parameters configurations. e) Modules accessibilities and rights.	User Management	• Reporting <-> Novel eDirectory • User <-> Authentication • User <-> User Management • Server Management <-> Novell eDirectory • User Management <-> Authentication	Pass
This test group comprises a series of test cases on TOE security functions for the administrator to configure and manage the TOE token user. The test will cover: a) Token user management. b) Access control rights.	Token Management & Cryptography	• Authentication <-> Novel eDirectory • User <-> Authentication • User <-> User Management • Token Management <-> Novel eDirectory • User <-> Token	Pass

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
		Management • User <-> Desktop Application • User <-> Mobile Application • Server Management <-> Novel eDirectory • Accounting <-> Authentication	
This test group comprises a series of test cases on TOE security functions to verify that the TOE is able to manage multiple ePassport authentication suite servers with a single console, whist handling the data import and export (backup and recovery) process towards the TOE.	Server Management	• User <-> User Management • Server Management <-> Novel eDirectory • User <-> Server Management	Pass

2.1.4.2 Penetration Testing

36 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.

37 From the vulnerability analysis, the evaluators conducted penetration testing to determine whether potential vulnerabilities could be exploited in the intended operating environment of the TOE, to attack performed by an attacker possessing a basic attack potential.

38 The penetration tests focused on:

a) Compromise the TOE Environment Configuration (IT Environment – Non-TOE Scope); and

b) Compromise administrator privilege by hacking the TOE.

39 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.

40 The results of the penetration testing note that a number of residual vulnerabilities exist that are dependent on additional resource, higher windows opportunity, longer duration to exploit, higher skill/knowledge or focused tools to be exploited. Therefore, 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 ePassport Suite v2.5 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

3 Results of the Evaluation

42 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of ePassport Suite v2.5 performed by CyberSecurity Malaysia MySEF.

43 CyberSecurity Malaysia MySEF found that ePassport Suite v2.5 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.

44 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

45 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.

46 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.

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

3.2 Recommendation

48 In addition to ensure secure usage of the product, below are additional recommendations for ePassport Suite v2.5:

a) Use it only in its evaluated configuration;

b) Configure the SSH port communication other than 22 and use higher bits of SSH encryption;

c) Users should use complex and mixture character password;

d) Enforce HTTPS encryption communication between TOE Administrator and TOE appliance.

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] EXTOL ePassport Suite v2.5 Security Target, v2.0, 30 June 2011.

[7] Evaluation Technical Report ePassport Suite v2.5, v1.5, 30 June 2011.

[8] ePassport Suite User Guide EC-5750-eP1000 (Standard Edition), v1.0, 27 October 2010

[9] ePassport Administrative Guide EC-5750-eP1000 (Standard Edition), v2.37, 27 October 2010

[10] ePassport Suite Installation Guide, v3.2, 27 October 2010

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
ISCB	Information Security Certification Body
LDAP	Lightweight Directory Access Protocol
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme

Acronym	Expanded Term
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
OTP	One-Time-Password
PP	Protection Profile
SOAP	Simple Object Access Protocol
SOUP	Simple Offline USENET Packet Format
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
2FA	Two-Factor Authentication

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.

Term	Definition and Source
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.

--- END OF DOCUMENT ---