Doc Ref RD/JL/069

Replaces: N/A

EXTOL ePassport Suite v2.5
Security Target v2.0

ECSB/MyCC/JL/002
Common Criteria EAL1 Certification

Extol Corporation (M) Sdn Bhd (121135-U)
Extol MSC Bhd (643683-U)
"Extol Group"
www.extolcorp.com
Unit G1, Ground Floor,
Wisma UOA Pantai,
No. 11, Jalan Pantai Jaya,
59200 Kuala Lumpur, Malaysia

CERTIFIED TO ISO/IEC 27001:2005
CERT NO. : AR 4223

CERTIFIED TO ISO 9001:2000
CERT NO. : AR 4480

Amendment Record

Version No.	Change Reference No.	Author	Published Date	Sections Changed	Description of changes	Page No
1.0	N/A	Mehmet & Wai	8 June 2010	N/A	Initial Document	All
1.1	**Error! Unknown document property name.**	Mehmet & Wai	25 June 2010	N/A	MySEF ERR#1	All
1.2	N/A	Mehmet & Wai	28 July 2010	All	Evaluator's comments and scope changes.	All
1.3	N/A	Mehmet & Wai	16 August 2010	All	Evaluator's comments after EPP	All
1.4	MySEF-3-EXE-E022-EOR01-d1	Mehmet & Wai	9 September 2010	All	Evaluator's comments after EOR 001	All
1.5	MySEF-3-EXE-E022-EOR02-d1	Mehmet & Wai	22 September 2010	All	Evaluator's comments after EOR 002	All
1.6	N/A	Mehmet & Wai	17 November 2010	All	Minor changes	All
1.7	N/A	Jackson	8 December 2010	TOE Type	Minor changes	6-8
1.8	N/A	Jackson	10 December 2010	SFR	Removed FAU_STG.4	All
1.9	N/A	Jackson	2 March 2011	SFR, TSS	Added descriptions fixed error and updates SFR's.	All
1.10	N/A	Jackson	3 March 2011	TSS	Added detail descriptions on the Table 10	All
2.0	N/A	Jackson	30 Jun 2011	SFR	Rearrange SFR	All

ABBREVIATIONS

Abbreviations	Descriptions
CC	Common Criteria for Information Technology Security Evaluation
CBC	Cipher Block Chaining (CBC)
EAL	Evaluation Assurance Level
ST	Security Target
SFR	Security Functional Requirements
OTP	One Time Password
TOE	Target of Evaluation
TSF	TOE Security Functions
SFP	Security Function Policy

SOAP	Simple Object Access Protocol
TSF	TOE Security Functions
SOUP	Simple Offline USENET Packet Format
YAST	Yet Another Setup Tool

Project ID: ECSB/MyCC/JL/002	
Project Name: Common Criteria EAL1 Certification	
Prepared By:	**Approved By:**
Name: Mehmet Cakir / Shang Ye Wai	Name: Jackson Lim
Date: 30 Jun 2011	Date: 30 Jun 2011

TABLE OF CONTENTS

INDEX OF TABLES

INDEX OF FIGURES

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 ST and TOE Identification

ST Title:	Extol ePassport Suite v2.5 Security Target
ST Version:	V2.0
TOE Software Identification:	ePassport Suite v2.5
Evaluation Assurance Level:	EAL 1
CC Identification:	CCMB-2009-07-001, CCMB-2009-07-002, CCMB-2009-07-003, CCMB-2009-07-004)

Table 1 ST and TOE Identification

1.2 Document 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 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**]”.

The outcome of the refinement operations are shown with ~~strikeout~~ onto the sentences or word, or amended with new sentences or words are shown in *italic*

1.3 TOE Overview

ePassport Suite is an Authentication System which supports a suite of authentication mechanisms to secure user accounts, intranet web apps and on-line transactions. The ePassport enabled Two-factor Authentication (2FA), requiring users to provide two means of authentication. The identification and authentication involve two attributes which are described as "something you know" and "something you have". Used in combination, these two factors will provide protection and security for any Internet transactions.

User names and passwords are commonly used in a traditional identification process. It is the one and only form of authentication, relying on the "something you know" attribute. The second form of authentication relies on the "something you have" attribute, usually a secret PIN or OTP generated by a user application or devices. The 2FA based OTP complements or strengthens the identification process. The OTP can be generated from application in mobile phones, software for desktops or hardware generators.

The ePassport Suite, which is installed behind an internet gateway firewall, is providing a secure remote access with security implementation of 2FA for the users. The users of the ePassport Suite could integrate any application which require authentication. Integrated systems, such as Active Directory, MySQL and others (refer to Figure 1 for further information) to the ePassport Suite can only be accessible by the users with a successful authentication.

Below stated the list of Security Features of the TOE:

Audit	Accounting and Reporting module inside the Management Console provides the scope of the reporting functionality. In addition to the regular system reports, the TOE provides system logs for the audit requirements defined in section TOE Summary Specification (TSS) in Security Target.
Authentication	Authentication to TOE is based on the user credentials and the authentication process that is performed by the core engine with supported by Tokens (Software desktops, Hardware Generator or Application in Mobile Phone) that generates OTP.
Cryptography	Cryptographic functions are performed by the cryptography module inside the core engine (refer to Figure 1 for further details).Also, the Tokens that generating OTP's are using the same cryptography algorithms perform by cryptography module of core engine. The detailed functionality is defined in TOE Summary Specifications.
Security Management	User, Token and Server management of the ePassport Suite are configured by the Administrators via the management console. Basically, the centralized management accessibility if TOE Administrators to perform maintenance, setting, configuration or any related functions for operation of TOE. The scope of the Management Console is defined in the Security Functional Requirements and TOE Summary Specifications in this ST.

Table 1 Security Features of the TOE

1.3.1 TOE Type

ePassport Suite is **a web based authentication system** which enables 2-Factor Authentication System on the login page.

Below is the list of non-TOE requirements:

#	Requirements	Descriptions	Version & Specifications
1	Hardware	1. Authentication Server 2. Storage 3. RAM 4. Processor 5. Monitor	1. Linux Server for installation; 2. 750 MB Disk Space for software, 750 MB Disk Space for user data 3. 512 MB SSH based Network for local installation, 512 MB VNC based network for graphical installation, 512 MB for installation via FTP. 4. Supported Processors; • AMD64 • IBM Power (IBM System i and IBM System p) • IBM System z (64-bit) Intel64 • Itanium Processor Family • x86 5. Acceptable resolution view based on monitor.
2	Software	1. Operating System 2. Database 3. Web Browser 4. Third party applications	1. Any operating system that supports JRE 1.6. 2. Database requirements; PostgreSQL 8.2 3. Supported Web Browsers; • IE 6 till IE8 • Firefox 2.5 till 3.6 • Chrome 5 till 8 4. iManager (2007)
3	Supporting Devices	1. Hardware generator 2. Software Desktop 3. Firewall	Any hardware generator and software desktop that supports JRE 1.6. Any type of firewall appliance that provide network security at the Internet gateway.
4	Supporting Systems	1. Novell eDirectory v8.5 and above. 2. SMS System 3. Secure SMS System 4. PKI and Digital Certificates.	N/A.

#	Requirements	Descriptions	Version & Specifications
5	Mobile Devices	1. Mobile Phones	Any device or system that supports JRE 1.6.
6	Integrated Applications/Systems	1. Biometrics 2. Server Management 3. IAG-MS 4. Active Directory 5. MySQL 6. Microsoft SQL Server.	All of these integrated application connected to the TOE via RADIUS, Web Services LDAP or JDBC.

Table 2 List of non-TOE requirements

1.4 TOE Description

1.4.1 Physical Scope of the TOE

The TOE is designed to provide customers with a token option of two-factor authentication. It is embedded software that leverages on the mobile devices as a hardware medium. The ePassport base systems consists of four major components as stated below, as illustrated in Figure 1;

a) Core Engine
b) Management Console
c) Type of Systems Integrated with ePassport.
d) ePassport Suite type of Applications, Certifications and Tokens.

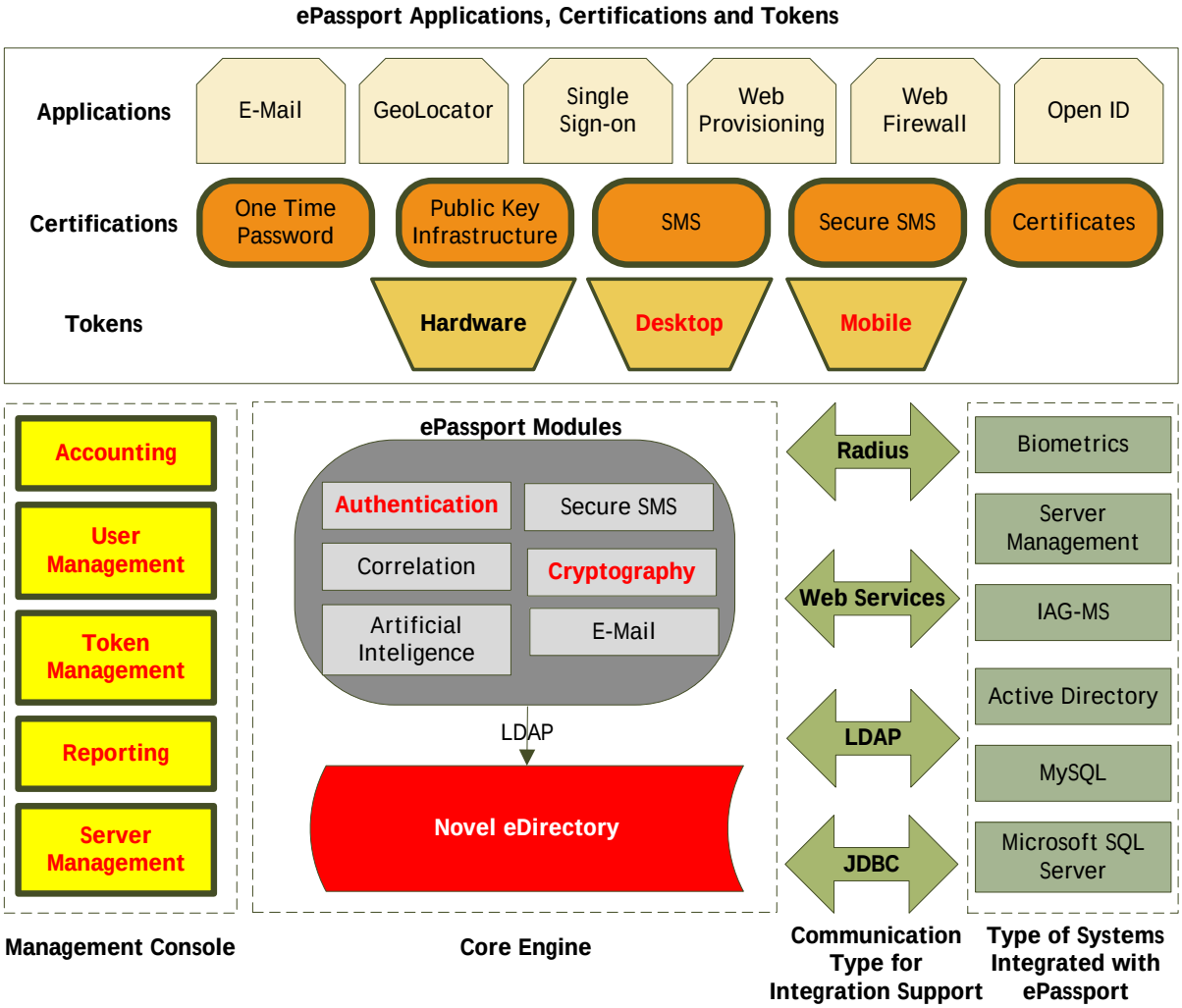

Figure 1 Structure of ePassport Suite

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

Core Engine	The core engine of the TOE is consisting of the ePassport Suite Modules which are the Authentication and Cryptography Modules. 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 in aspects of handling the information related to TOE operation and data.
Management Console	Management Console of the TOE is the configuration 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.
Type of Systems Integrated with	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

ePassport Suite	Services, JDBC and LDAP.
ePassport Suite type of Applications, Certifications and Tokens.	List of applications, certifications and tokens that can be used with ePassportSuite 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).

Table 3 Components of ePassport Suite

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 and outside of the network.

The hardware includes authentication server appliance, storage, RAM, processor and display monitor are treated as IT environment and not in the scope of the evaluation.

List of software includes, which is the operating system, database, web browsers, Supporting Systems (Novell eDirectory) and any kind of the integrated applications/systems where the TOE provides authentication support are treated as IT environment and not in the scope of the evaluation.

The services provided by ePassport Suite to the desktop and mobile users are configured and maintained by two types of users. The main user role is named as “Administrators” who has all the administrative rights in the Management Console. Other than Administrators, which is, new system groups and new system users assigned to these system groups can be created and provided with appropriate access rights can be given to these new users. Throughout this ST users who do not have administrator rights are referred as “System Users.” Also, other users that have not assigned to system groups or known as system users and accommodate with tokens, are known as Token Users.

ePassport Suite provides security enforcement as in Two-Factor Authentication (2FA), by requiring users to key in username, password and random number generated (OTP) from these tokens; ePassport Suite Hardware generator, ePassport Suite software desktops or ePassport Suite application in mobile phone. If the process authentication is successful, users will allow accessing the intranet web apps protecting from threats of password key logger.

ePassport Suite were accessible by Administrators by enforcement of 2FA without requirements of random number generated (OTP). However, Token Users were assigned with dedicated token, registered and enable by Administrators. Unlike users of ePassport Suite, Administrators will be redirect to the Management Console as in TOE management system for Administrators. Token Users other than Administrators will be redirected to the web resources assigned to them. Management Console is a centralized management of TOE in terms of logs auditing, user management, server management, token management,

managing integrated systems, databases management and arranging communications supports.

ePassport Suite provides an operational user guide and preparative procedures to its customers, which guide them to install and start-up the TOE according to the requirements and also to use them according to the proper guidance.

Below is illustration of TOE in aspects of physical scope:

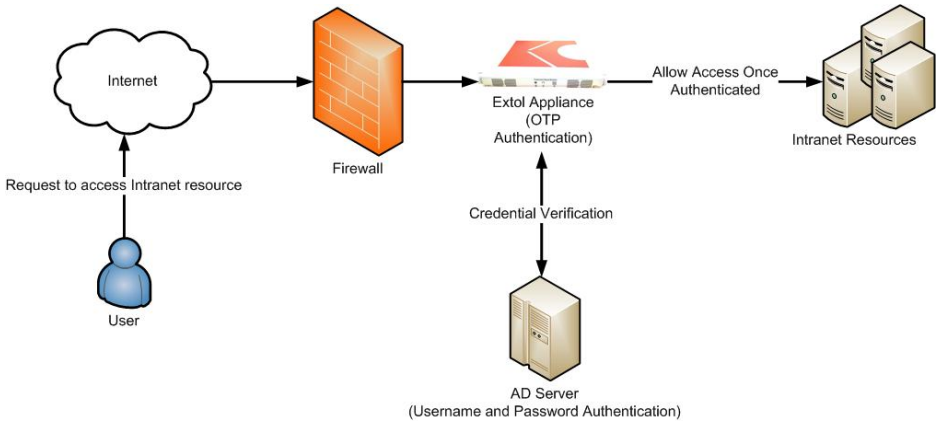

Figure 2 Physical Scope of TOE

- Notes on Figure 2: ePassport Suite shall be distributed by developer in aspects of appliance or software based, installed and configured by EXTOL developer for the client.
- Notes on Figure 2: AD (Active Directory) is a centralized system that provided management of network users; that stores all user credentials including username and password. AD is not provided by EXTOL developer, which is already implemented in the client site.
- Notes on Figure 2: Administrators are allowed to access the TOE from the intranet network. Administrators were not allowed to remotely access the TOE from external network (Internet) even using VPN connections.

1.4.2 Logical Scope of the TOE

1.4.2.1 Audit

Below are the components involved in Audit features.

Accounting (Management Console)

Management console capture logs for system wide changes (overall changes happening on the ePassport Suite), authentication attempts and system status. Method to access each of the logs and its description are explained in great detail in the operational user guidance. Each of the logs is stored in the Postgres database (provided by Novell's eDirectory system in Core Engine) and it is password protected.

Reporting (Management Console)

ePassport Suite installed in an appliance or client server, that is supporting logs accounting, where logs are presented on the Management console via reporting module. When the Management Console requests the logs information out from Postgres database (Novell's eDirectory system), it will send service request via internal communication platform between Management Console and Core Engine. The functions of reporting module is to represent the logs in graphical information easily capture by Administrators and exports in printable formats.

1.4.2.2 Authentication

Below are the components involved in Authentication features.

Authentication Module (Core Engine)

The Authentication module is used by the Administrators at Core Engine to configure administrative setting for the token users. Administrators will first accessing the Management Console and there will be a link to the Authentication Module setting via web browser.

The Core Engine Authentication module is used to check the user's credential to identify user's access right. The credential is stored at the Novell's eDirectory, along with user's access right, policy, and other related information about the user. When the user key in their username and password, the front end will send the credential in encrypted (provided by IT environment) format to the backend by using supported communication type based on integration systems, then one or more of integration systems will send the authentication request to the Novell eDirectory via LDAP communication protocol. If the username and password matched, the flow is reversed, and then the identification and authentication query will be hold for token verification.

Next, the Authentication module is used to check token users credential according to the authentication method assigned to them. There is several multiple token authentication method available for users. The description for each authentication method is explained at the operational user guidance. For example: when user key

in their username, password and OTP on the web browser (web application), username and password is sent to a database for verification. Once username and password are verified, the web application will send the OTP to the ePassport Suite server for authentication process. Once the ePassport Suite Authentication module receives the OTP request, it will check its internal algorithm for verification. Once authenticated, the ePassport Suite server will send an appropriate response to the web application. Then the web application will allow the user to enter the Intranet resources, which is assigned to that user. As for Administrators, the request will be directed to the Management Console.

Tokens (ePassport Suite Tokens)

When user key in their OTP on the login page, OTP sequence number is sent to TOE through SOAP where it is a protocol specification for exchanging structured information in the implementation of Web Services in computer networks. Then the communication will pass the OTP to the authentication module for verification. The authentication module will compare the OTP number with the master list to check whether it matched, and whether that number falls within the predesignated numbers. If no match was found, or the number falls beyond the predesignated numbers, a fail response will be sent to the communication module, and that communication module will pass the message to the login page via SOUP. There are two types of Tokens that declared inside the scope of TOE:

- Desktop Machine Software (Desktop Software Token); and
- Mobile Phone Application (Mobile Phone Token).

Note: Hardware Token is not part of the TOE scope.

1.4.2.3 Cryptography

Below are the components involved in Cryptography feature of Logical Scope.

Cryptography Module (Core Engine)

The Cryptography module is used in ePassport Suite application for mobile phones token, ePassport desktop software token, and ePassport Suite licensing function. Kindly refer to the figures located in section 5.1.3 for the in-depth cryptography implementation for each of the functions.

In mobile and desktop tokens, the cryptography module is mainly used for token registration and OTP generation. In the ePassport Suite licensing function, cryptography module is used to encrypt the licensing file itself from unauthorized editing.

The same processes were done in the ePassport Suite Cryptography module within the ePassport Suite server. All the tokens are not linked in aspects of online synchronization or having any type of communications between ePassport Suite servers. ePassport Suite can be established in several appliance, known as ePassport Suite servers, which is link to each other via network in aspects of operations but not generating OTP. Each of them are generating the random numbers separately, and ePassport Suite server have its own mechanism to verify the generated random number generate by all the tokens.

Tokens (ePassport Suite Tokens)

During the registration process, the user enters a sequence of numbers to the OTP token, that sequence of number is provided by the ePassport Suite server and it will be the input for the OTP Generator. OTP generator is an in house hashing algorithm that utilize AES encryption algorithm to generate sequence of number. AES key (16 bytes) is provided by the Secure Random class and it is an in house pseudo random generator. It extends Java's Random class. It uses AES algorithm to generate the final pseudo random number. UserID (16 bytes) is used as the AES key. The end result is the OTP number is generated.

1.4.2.4 Security Management

Below are the components involved in Security Management feature of Logical Scope.

User Management module (Management Console)

Users that have intention of accessing the Intranet resources must be given an access right by the Administrators before they are allowed to enter. Users also able to access the Management Console if they granted a customs privilege to view content of the Management Console. The user policy can be managed in the User Management module, where the Administrators can add, modify and delete users and their privilege. Furthermore, Administrators have capability to manage group and user's role. Administrators are able to group the users with similar roles, fine-tuning the access right for all the users that belongs to a particular group. Also, Administrators could assign the session time of each user as individual or as a group.

All users' information is stored in the Novell eDirectory. In order to view user related information in Management console, web service request shall be invoked to extract the data from Novell eDirectory via the LDAP. Access Control of the users is managed by the TOE according to the access rights defined in LDAP.

Token Management (Management Console)

Administrators can manage (add, modify and delete) token users via the Management console. Administrators can also add authentication function for each token user; for example, token user A is assigned with Hardware generator OTP and token user B is assigned with desktops software OTP.

Token users' information is stored in the Novell eDirectory. In order to view user related information in Management console, web service request shall be invoked to extract the data from Novell eDirectory via the LDAP.

Server Management (Management Console)

Management console is able to manage multiple ePassport Suite authentication servers with a single console. Each of the information related to the authentication server is stored in the Novell eDirectory. Basically, ePassport Suite server able to be establishes and well setup in multiple appliance within single network or located elsewhere in different network. Generally, ePassport Suite can be globally setup anywhere.

2 Conformance Claims

This ST and TOE are conformant 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.
- The Security Target (ST) is package-conformant to Evaluation Assurance Level 1 (EAL 1).
- The Security Target (ST) did not conformant to any Protection Profile (PP).

3 SECURITY OBJECTIVES

This section defines the security objectives for the Operational Environment of the TOE.

3.1 Security Objectives for the Operational Environment

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

Security Objective	Description
OE.INSTALL	The TOE shall be delivered, installed and managed by responsible authorized personnel.
OE.PPROTECTION	The TOE must be kept in a physically secured location to prevent attacker from accessing the TOE physically.
OE.NOEVIL	Administrators and Users are non-hostile, appropriately trained, and follow all user guidance, installation guidance and configuration guidance.
OE.TIME	The operational environment shall provide a reliable date and timestamp from trusted source known by Administrators of the TOE.
OE.RELIABLE	All hardware and 3rd party software supporting the TOE are updated, reliable and operating in good conditions.

Table 4 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 Component 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. 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.

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_EXT.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 NTP Server.

4.1.2 Security Audit Generation

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

Requirement Class	Requirement Components
FAU: Security Audit	FAU_GEN_EXT.1 Audit data generation

FAU class contains requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types. The following extended requirement for the FAU class has been included in this ST because the operational environment is capable of providing security audit generation for TSF functions.

FAU_GEN_EXT.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM_EXT.1 Reliable time stamps

FAU_GEN_EXT.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) [**events listed in the Table 5 List of Audited Events**]

Audited Events	Related SFR	Description
Successful Log on	FIA_UAU.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
Session Time Out	FTA_SSL.1	User session time-out

Table 5 List of Audited Events

FAU_GEN_EXT.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.

Application Note: Under component FAU_GEN.1.1, item (a) are removed due to the TOE did not provided functionality of start up or shutdown of audit fundtions. This because of the audit function operates automatically with the TOE during startup and shutdown. No manually overwrite start up or shutdown audit functions are located.

4.2 TOE Security Functional Requirements (SFRs)

Requirement Class	Requirement Component	Dependencies
FAU: Security Audit	FAU_GEN.2	FAU_GEN_EXT.1, FIA_UID.1
	FAU_SAR.1	FAU_GEN_EXT.1
	FAU_SAR.2	FAU_SAR.1
	FAU_STG.1	FAU_GEN_EXT.1
FCS: Cryptographic Support	FCS_CKM.1/Crypto	FCS_CKM.2 or FCS_COP.1 ,FCS_CKM.4
	FCS_COP.1/Crypto	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4
	FCS_CKM.1/Token	FCS_CKM.2 or FCS_COP.1 ,FCS_CKM.4
	FCS_COP.1/Token	FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1, FCS_CKM.4
FDP: User Data Protection	FDP_ACC.1	FDP_ACF.1
	FDP_ACF.1	FDP_ACC.1, FMT_MSA.3
	FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1
	FDP_IFC.1	FDP_IFF.1
	FDP_IFF.1	FDP_IFC.1, FMT_MSA.3
	FDP_ITC.1	FDP_ACC.1 or FDP_IFC.1, FMT_MSA.3
FIA: Identification & Authentication	FIA_AFL.1	FIA_UAU.1
	FIA_ATD.1	No Dependencies
	FIA_SOS.1	No Dependencies
	FIA_UAU.2	FIA_UID.1
	FIA_UAU.6	No Dependencies
	FIA_UID.2	No Dependencies
	FIA_USB.1	FIA_ATD.1
FMT: Security Management	FMT_MOF.1	FMT_SMR.1, FMT_SMF.1
	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_MTD.1	FMT_SMR.1, FMT_SMF.1
	FMT_SMF.1	No Dependencies
	FMT_SMR.1	FIA_UID.1

Requirement Class	Requirement Component	Dependencies
FTA: TOE Access	FTA_MCS.1	FIA_UID.1
	FTA_SSL.1	FIA_UAU.1
	FTA_TAH.1	No Dependencies

Table 6 List of SFRs

4.2.1 Security Audit

4.2.1.1 FAU_GEN.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.

4.2.1.2 FAU_SAR.1: Audit Review

FAU_SAR.1.1 The TSF shall provide [**administrators**] 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.

Application Note: The list of audited events is shown in the Table 8 and the types of logs are shown in Section 5.1.1.

4.2.1.3 FAU_SAR.2: 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.

Application Note: Log type is the description of type of log bound with events as described in Table 8 in Section 5.1.1.

4.2.1.4 FAU_STG.1: Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [**prevent**] unauthorised modifications to the stored audit records in the audit trail.

4.2.2 Cryptographic Support

4.2.2.1 FCS_CKM.1/Crypto: Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES, CBC, Secure Random**] and specified cryptographic key sizes [**16 bytes**] that meet the following: [**none**].

Application Note: The dependency for the functional component FCS_CKM.4 is not met inside the TOE because the cryptographic algorithms which are explained under the TSS section in detail are only used for keys generation. So keys generated are used as encrypted user ids. That's why secure key

destruction is not a requirement for TOE and the TOE does not conduct key destruction.

Java uses automated garbage collection in order to destroy the generated keys. For further clarification, kindly refer to the following wiki: http://en.wikipedia.org/wiki/Garbage_collection_(computer_science)

Application Note: Secure Random is an extension of Java standard Random class. The Java Random class generates a stream of pseudorandom numbers based on the output of an AES/CBC encryption. The class uses a 48-bit seed, which is modified using a linear congruential formula. The AES/CBC gets its SecretKey, PlainText, and InitializationVector (IV) from an instance Java Random class. So in a nutshell, Java Random (user ID as seed) generates SecretKey, PlainText, and IV for use with an AES/CBC algorithm which then generates a series of encrypted binary data. This binary data is then converted into a stream of numbers using a Base96 encoder. Base96 shares the same concept with the standard (and well-known) Base64 encoding.

4.2.2.2 FCS_COP.1/Crypto: Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [**User ID Encryption**] in accordance with a specified cryptographic algorithm [**AES, CBC, Secure Random**] and cryptographic key sizes [**16 bytes**] that meet the following:[**none**]

Application Note: The dependency for the functional component FCS_CKM.4 is not met inside the TOE because the cryptographic algorithms which are explained under the TSS section in detail are only used for key generation. So keys generated are used as encrypted user ids and stored but not deleted. That's why secure key destruction is not a requirement for TOE and the TOE does not conduct key destruction.

Java uses automated garbage collection in order to destroy the generated keys. For further clarification, kindly refer to the following wiki: http://en.wikipedia.org/wiki/Garbage_collection_(computer_science)

4.2.2.3 FCS_CKM.1/Token: Cryptographic Key Generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES, CBC, Secure Random**] and specified cryptographic key sizes [**16 bytes**] that meet the following: [**none**].

Application Note: The dependency for the functional component FCS_CKM.4 is not met inside the TOE because the cryptographic algorithms which are explained under the TSS section in detail are only used for key generation. So keys generated are used as encrypted user ids and stored but not deleted. That's why secure key destruction is not a requirement for TOE and the TOE does not conduct key destruction.

Java uses automated garbage collection in order to destroy the generated keys. For further clarification, kindly refer to the following wiki: http://en.wikipedia.org/wiki/Garbage_collection_(computer_science)

4.2.2.4 FCS_COP.1/Token: Cryptographic Operation

FCS_COP.1.1 The TSF shall perform [**User ID Encryption**] in accordance with a specified cryptographic algorithm [**AES, CBC, Secure Random**] and cryptographic key sizes [**16 bytes**] that meet the following:[**none**]

Application Note: The dependency for the functional component FCS_CKM.4 is not met inside the TOE because the cryptographic algorithms which are explained under the TSS section in detail are only used for key generation. So keys generated are used as encrypted user ids and stored but not deleted. That's why secure key destruction is not a requirement for TOE and the TOE does not conduct key destruction.

Java uses automated garbage collection in order to destroy the generated keys. For further clarification, kindly refer to the following wiki: http://en.wikipedia.org/wiki/Garbage_collection_(computer_science)

4.2.3 User Data Protection

4.2.3.1 FDP_ACC.1: Subset Access Control

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

[

List of Subjects;

- **Administrators**
- **System Users associated to defined System Groups**

List of Objects
webconsole login
superuser all
system_configs view
system_configs add
system_configs edit
system_configs delete
system_groups view
system_groups add
system_groups edit
system_groups delete
system_logs view
system_users view
system_users add
system_users edit

List of Objects
system_users delete

].

4.2.3.2 FDP_ACF.1: Security Based Access Control

FDP_ACF.1.1 The TSF shall enforce the [**access control policy**] to objects based on the following: [**user identity and group membership(s) associated with a subject**].

Application Note: Access control policy inside the TOE is applied to the users according to the system groups that they have belong and their rights to access subjects within the TOE. When a user identifies his/her User ID and Password, TOE confirms the access rights of the user from LDAP according to its group memberships. Afterwards the user can only access the portions of the TOE which he/she have right to do.

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 denied**

].

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**].

Application Notes: The TOE provides the Administrators to define new user groups and associate access rights to these defined user groups. The Administrators will then create a new user and relate the user to a defined user group. TOE also allows Administrators to modify the access rights of a user. After the creation of the user, the TSF enforce access control policy according to the defined access rights of the user.

4.2.3.3 FDP_ETC.1: Export of User Data without Security Attributes

FDP_ETC.1.1 The TSF shall enforce the [**access control policy**] when exporting user data, controlled under the SFP(s), outside of the TOE.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

Application Notes: Exporting user data from TOE is subject to an access control. Only the users with appropriate access rights can get the system logs or configuration files by generating .pdf or .csv formatted files.

4.2.3.4 FDP_IFC.1: Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the [**information flow control policy**] on [**subject, objects, operations and information listed in Table 10**].

4.2.3.5 FDP_IFF.1: Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the [**information flow control policy**] based on the following types of subject and information security attributes: [**List of subject, object and information listed on Table 10**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**The operations are under the scope of information flow control Table 10**].

FDP_IFF.1.3 The TSF shall enforce the [**none**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**operations listed in the information flow control Table 10].**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**operations requests except the information flow control Table 10**].

Application Notes: The events that are under the scope of the information flow control are listed in Section 5 Table 10.

4.2.3.6 FDP_ITC.1: 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: [**none**].

Application Notes: Importing user data from TOE is subject to an access control. Only the users with appropriate access rights can retrieve system logs or configuration files from outside the TOE.

4.2.4 Identification and Authentication

4.2.4.1 FIA_AFL.1: Authentication Failure Handling

FIA_AFL.1.1 The TSF shall detect when [**Administrators configurable positive integer within** [**3 to an integer defined by Administrators**]] unsuccessful authentication attempts occur related to [**Administrators and User authentication**].

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

4.2.4.2 FIA_ATD.1: User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user ID, password, and OTP generator**].

4.2.4.3 FIA_SOS.1: Verification of Secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet [**minimum password length and password complexity set by the Administrators**].

4.2.4.4 FIA_UAU.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.

4.2.4.5 FIA_UAU.6: Re-Authenticating

FIA_UAU.6.1 The TSF shall re-authenticate the user under the conditions [**session time out**].

4.2.4.6 FIA_UID.2 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.

4.2.4.7 FIA_USB.1 User-subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**user ID, password and OTP generated**].
FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [

- **Input the User ID associate to the User and Administrators; and**
- **Input the password assciate to the User and Administrators; and**
- **Generate one OTP at one time by using Token associate with the User and Administrators; and**
- **Input the OTP that has been generated**].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**none**].

4.2.5 Security Management

4.2.5.1 FMT_MOF.1: Management of Security Functions Behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to [**disable, enable**] the functions [**access control rights**] to [**Administrators**].

4.2.5.2 FMT_MSA.1: Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [**access control policy**] to restrict the ability to [**query, modify**] the security attributes [**view system logs, add/delete/modify users, password, tokens**] to [**Administrators**].

4.2.5.3 FMT_MSA.3: 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 [**Administrators**] to specify alternative initial values to override the default values when an object or information is created.

4.2.5.4 FMT_MTD.1: Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to [**query**] the [**system logs**] to [**Administrators**].

4.2.5.5 FMT_SMF.1: Specification of Management Functions

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

system_configs view
system_configs add
system_configs edit
system_configs delete
system_groups view
system_groups add
system_groups edit
system_groups delete
system_logs view
system_users view
system_users add
system_users edit
system_users delete

].

4.2.5.6 FMT_SMR.1: Security Roles

FMT_SMR.1.1 The TSFshall maintain the roles [**administrator, users (associated to a defined user group)**].

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

4.2.6 TOE Access

4.2.6.1 FTA_MCS.1: Basic Limitation on Multiple Concurrent Sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [**0**] sessions per user.

Application Note: By default, there is not any limitation for the multiple concurrent sessions for the users; however the Administrators could limit the number via management console.

4.2.6.2 FTA_SSL.1: TSF Initiated Session Locking

FTA_SSL.1.1 The TSF shall lock an interactive session after [**1-30 minute**] by:
a. Clearing or overwriting display devices, making the current contents unreadable;
b. Disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [**re-authentication**].

4.2.6.3 FTA_TAH.1: TOE Access History

FTA_TAH.1.1 Upon successful session establishment, the TSF shall display the [**date, time**] of the last successful session establishment to the *Administrators*.
FTA_TAH.1.2 Upon successful session establishment, the TSF shall display the [**date,time**] of the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the last successful session establishment.

FTA_TAH.1.3 The TSF shall not erase the access history information from the *Administrators* interface without giving the *Administrators* an opportunity to review the information.

4.3 TOE Security Assurance Requirements (SARs)

Requirement Class	Requirement Component
ADV: Development	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 - conformance
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 7 List of SARs

5 TOE SUMMARY SPECIFICATIONS

5.1 TOE Security Functions

5.1.1 Audit (Accounting and Reporting Module – Management Console)

The following system logs are created and stored in the TOE. In addition to the following audit logs, the TOE can be configured for taking the server logs from the operating system if requested. Below is the list of log types that the TOE generates:

Log type	Description of Events
Failure	• Any failed activity performed by the user is listed under this category. o System user session is timed out o System user is disabled due to excessive password attempt o Wrong password is entered for the username
Success	• Any successful activities performed by the system user is listed under this category o User is logged in successfully o Security group is added, deleted and updated successfully o Password policy is configured successfully o User is added, deleted and updated successfully
Information	• ePassport Suite Administrators may retrieve critical information from this log type. o Time when a ePassport Suite component is up o Amount of time that a component is down o When the Administrators logged out from the system
Error	• Any system level error is listed under this category, which includes system components and system users. o Time when ePassport Suite component is down o Which ePassport Suite component is down o Logout error

Table 8 Log Types

All log types are associated with type, date and time of an event and all events are associated with the users that cause the event.

Administrators may select the set of event to be audited. Only Administrators can view the system logs. Logs cannot be deleted and modified from the database by anyone except for administrators.

When the memory of the log storage in the Postgres database is full, then the system starts to overwrite the first log in order to store the incoming new logs.

Besides the accounting logs of the audit function the TOE also provides reporting logs which is provided via the reporting module. These logs are generated and stored in the same

database with the audit logs however they are generated for system monitoring and maintenance.

Date and time data of all the audit logs are received from a reliable NTP server which is accepted as an extended security function.

This Security Function is providing the following functional requirements;
FAU_GEN_EXT.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_STG.1, FPT_STM_EXT.1

5.1.2 Authentication

5.1.2.1 Authentication Module (Core Engine)

The Administrators and User authentication and identification processes to the TOE is subjected to an authentication module. Upon creation of a user by Administrators, which is assigned to a specific user group and associated with access rights, the users can connect to the TOE via web browser login page; provided with prompted request of user id, password and OTP in order to conduct any actions within the TOE or accessing intranet resources. During the authentication process, unsuccessful attempts are controlled and the system provides limited information (i.e. error during the authentication process is not provided in detail) to the user. The processes of authentication and identification has provided in Section 1.4.2.2, explained at paragraph 4.

The user passwords can be configured according to their length and password complexity by the Administrators. The TSF enforces users to provide passwords which comply with the specification (set by Adminisrators).

The authentication module enforces users to re-authenticate when the sessions are automatically locked after a user configured period of time has passed.

5.1.2.2 Tokens (ePassport Suite Tokens)

Authentication module of the TOE is also controlling the authentication support for the ePassport Suite Tokens. The OTP generated by the tokens are sent to the authentication module via the communication module and Authentication module and Cryptography module collaborate in verification the user generated OTP's in order to allow users to access the supported applications (such as biometric, server management and etc. Refer to Figure 1) or intranet resources. Either a pass or a fail response sent to the communication module after a check within the master list (within the predesignated number) if the OTP number is correct or not.

This Security Function (Authentication Module and Tokens) is providing the following functional requirements

FIA_AFL.1, FIA_ATD.1, FIA_SOS.1, FIA_UAU.2, FIA_UAU.6, FIA_UID.2 and FIA_USB.1

5.1.3 Cryptography

The following cryptographic operations are conducted with the crypto functions of the TOE;

5.1.3.1 Cryptography Module (Core Engine)

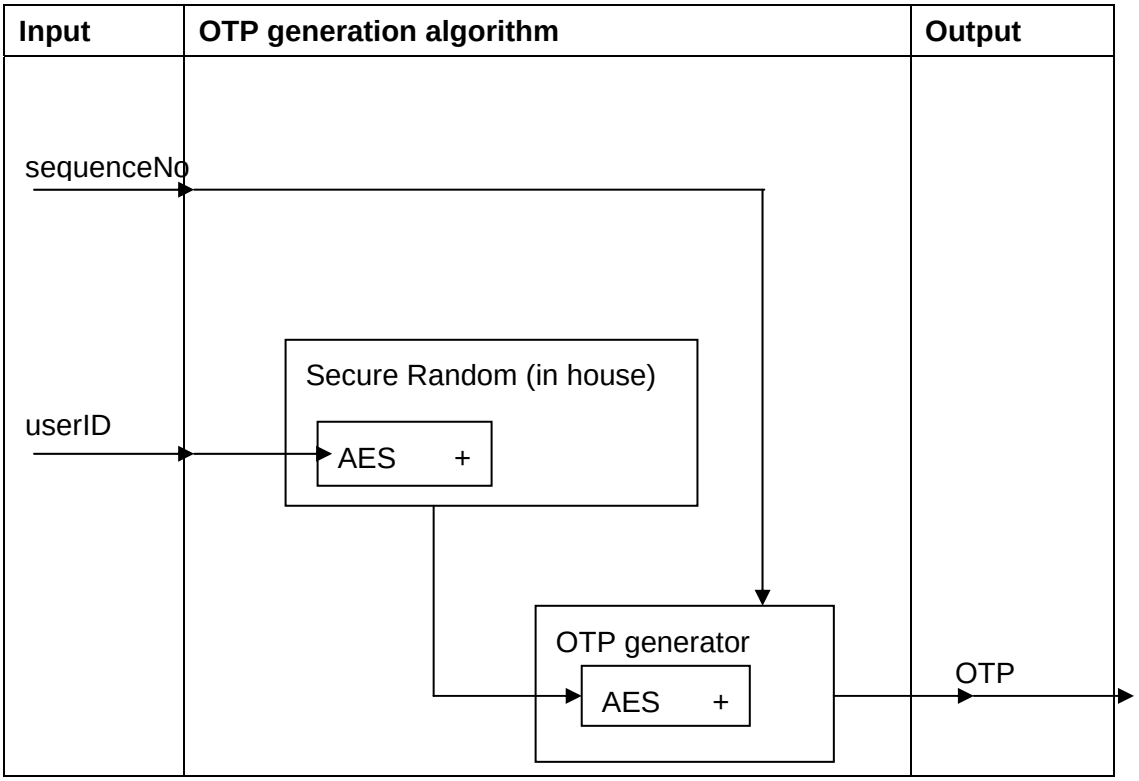

Figure 3 Process flow of OTP generation on server

Generation of OTP's as random numbers by ePassport Suite server/servers is used for comparison of OTP generated by the tokens. All the OTP's, which is referring as master list stored inside the ePassport Suite database handled by Novel eDirectory service.

Referring to Figure 3, the AES/CBC is AES algorithm in CBC mode. The SecureRandom class is a pseudorandom generator and uses user ID's as seed. The SecureRandom pseudorandom generator is used to generate the keys for the next module which is the OTP generator. A 128-bit random key generated from SecureRandom is used as the SecretKey/IV for the next AES/CBC initialization (in OTP generator module). This AES/CBC (OTP generator) then takes the sequence number and encrypts it to generate a series of encrypted binary data, which is then converted into OTP using Base96 encoding. All these OTP's will be stored inside the database handle by the Novel eDiretcory service.

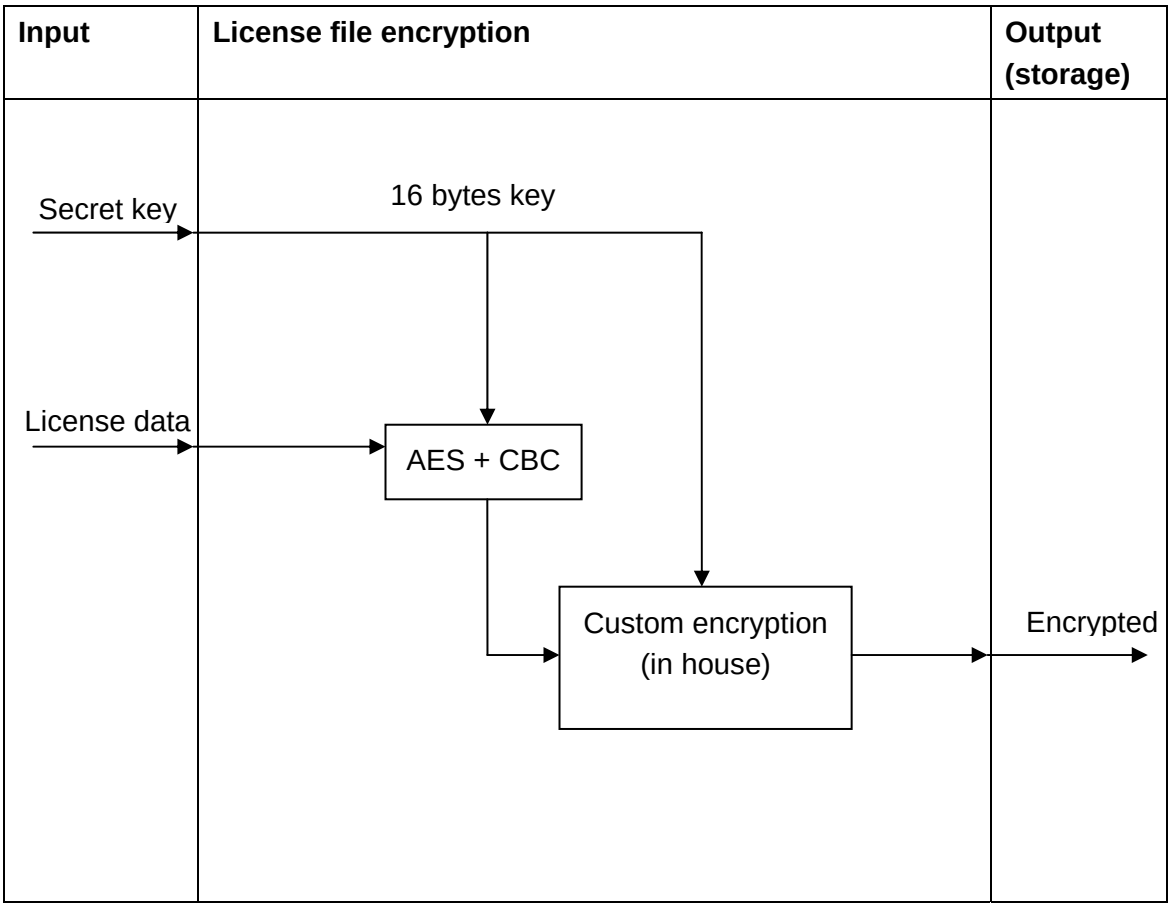

Figure 4 Process flow of license file encryption

Referring to Figure 4, the AES/CBC is AES algorithm in CBC mode. The secret key is a 128-bit key which exists in the ePassport Suite server only. The first process is to encrypt the license information using AES/CBC, by using 128-bit secret key for both SecretKey and IV. Next, the encrypted output is then further jumbled using a custom made encryption algorithm, developed by EXTOL in house algorithm.

During the OTP generation, the OTP value is stored in a Java variable. Each variable has its own space in RAM and that RAM is cleaned periodically and automatically by Java Garbage Collector. The variable is then displayed to the user. If the OTP value change, the value in the variable will change.

Thus the dependence to the cryptographic key destruction is not met by the TOE, since the algorithms are used to create random numbers but not for encrypting and decrypting plain texts. That's why the TOE stored the cryptographic secret key (single key for one ePassport Suite) and do not need to destruct them.

This Security Function (Cryptography Module) is providing the following functional requirements;

FCS_CKM.1/Crypto and FCS_COP.1/Crypto

5.1.3.2 Tokens (ePassport Suite Tokens)

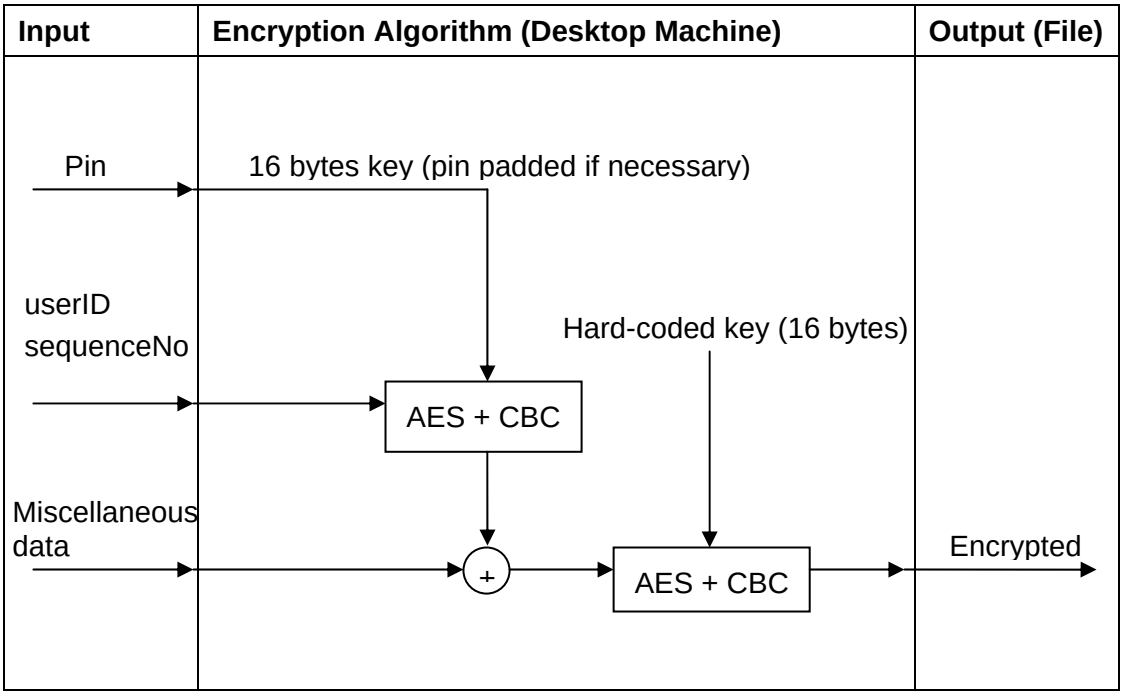

Figure 5 Process flow of OTP generation on desktop machine

Referring to Figure 5, the AES/CBC is AES algorithm in CBC mode. AES/CBC uses the 128-bit (16 bytes) Pin for both SecretKey and Initialization Vector (IV). If Pin is disabled, a hard-coded Pin will be used for encryption. If Pin is enabled manually by the user, the user will have to provide the Pin each time the desktop machine application is launched.

Based on Figure 5, the miscellaneous data, which is provided by the software, contains information of application version, Pin availability, and activation status; which is used part of seed during cryptography processes.

The first part is to encrypt user id and sequence number information which can only be decrypted back if the original Pin provided by the user is used. The next step is combining this already encrypted data with other less sensitive information such as program version, activation status and Pin availability. This combined data is then further encrypted using another instance of AES/CBC encryption with a hard-coded SecretKey and IV – different than the Pin given by the user. The final output is then saved into a configuration file at the user's home directory.

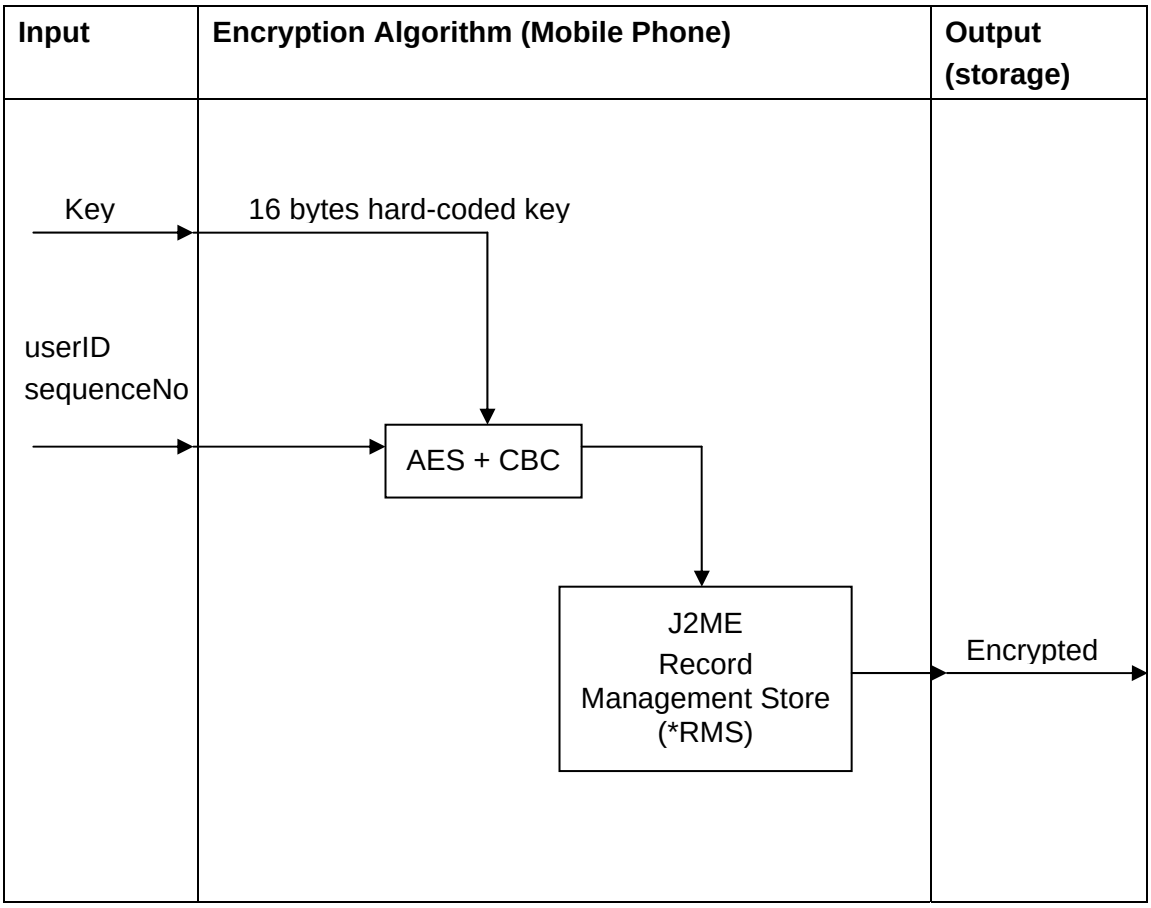

Figure 6 Process flow of OTP generation on mobile phone

Referring to Figure 6, the AES/CBC is AES algorithm in CBC mode. Both SecretKey and IV are already hard-coded into the mobile application itself. The user id and sequence number information is then encrypted using AES/CBC and stores the output into J2ME RMS storage. The J2ME RMS is a Java standard interface for storing data in mobile phones. J2ME RMS states that no other application will have access to the data except for the application that created it in the first place.

During the OTP generation, the OTP value is stored in a Java variable. Each variable has its own space in RAM and that RAM is cleaned periodically and automatically by Java Garbage Collector. The variable is then displayed to the user. If the OTP value change, the value in the variable will change.

Thus the dependence to the cryptographic key destruction is not met by the TOE, since the algorithms are used to create random numbers but not for encrypting and decrypting plain texts. That's why the TOE stored the cryptographic secret key (single key for one ePassport Suite) and do not need to destruct them.

This Security Function (Tokens) is providing the following functional requirements; FCS_CKM.1/Token and FCS_COP.1/Token

5.1.4 Security Management

5.1.4.1 User Management (Management Console)

The Administrators of the TOE can configure the Security Management functions of the TOE with the Management Console. The Administrators can manage the users, assign access rights and manage user accounts with the Management console.

The Management console allows the TOE Administrators to authorize other users to access the ePassport Suite Management GUI via web browser.

Once the user has been added successfully in the system, a dialog message appears at User Management console, and the newly added username appears in the System Users' table. This table is in the management console where the Administrators can review the system users. The Administrators may then further segregate the users according to roles and rights shown in Table 9. These access rights can be associated either to a user group or a specific user.

Module rights	Description
webconsole login	• This is for system users to login to ePassport Suite GUI • If the system users are not assigned with this right, they can't log in to the ePassport Suite administrator GUI.
superuser all	• Once the user is assigned with the "superuser all" right, it overrides all previously assigned rights and this user inherits the capability of an Administrator with privileges of superuser, defines that ability to perform modification without any reviews of actions. • This user has access to all the functions in ePassport Suite administrator GUI.
system_configs view	• This is for managing system configuration with the ability to view. • This is a prerequisite for all "system_configs" related rights. When this right is not assigned to the user, the user is not able to view the system configuration module.
system_configs add	• This is for managing system configuration with the ability to add.
system_configs edit	• This is for managing system configuration with the ability to edit.
system_configs delete	• This is for managing system configuration with the ability to delete.
system_groups view	• This is for managing system groups with the ability to view. • This is a prerequisite for all "system_groups" related rights, when this right is not assigned to the user; the user is not able to view the system group's module.

Module rights	Description
system_groups add	• This is for managing system groups with the ability to add.
system_groups edit	• This is for managing system groups with the ability to edit.
system_groups delete	• This is for managing system groups with the ability to delete.
system_logs view	• This is to allow users to view system logs.
system_users view	• This is for managing system users with the ability to view. • This is a prerequisite for all "system_users" related rights. When this right is not assigned to the user, the user is not able to view the system user's module.
system_users add	• This is for managing system users with the ability to add.
system_users edit	• This is for managing system users with the ability to edit.
system_users delete	• This is for managing system users with the ability to delete.

Table 9 Access Rights

Information Flow Control Policy is the security functionality which enforces "Administrators" to access a specific list of objects and conduct a defined list of events. The following list is listing the subject-object and event mapping which is under control of the information flow.

Notes: Information flows are managed by the Core Engine of ePassport Suite, which are internal processing capabilities of eNovel Directory, Postgress database and programming modules of ePassport Suite.

Subject	Object	Operations	Information
Administrators	Change IP Address	• Key in username • Key in password • Press the enter key • Modify IP in "YAST"	• Username • Password • IP in YAST
Administrators	Log-in	• Key in username • Key in password • Click on the login button	• Username • Password
Administrators	Monitor system status	• View server status • View component status • Click on server IP address • View live active request graph • View live throughput graph • View live average	• Server Status • Component Status • Active Request Graph • Live Througput Graph • Live Average Processing Time

Subject	Object	Operations	Information
		processing time • View CPU utilization over time • View memory utilization over time	• CPU Utilization • Memery Utilization
Administrators	Add system user	• Click on "System users" link • Click "Create New User" button • Key in username and password for the new user	• List of System users • Username • Password
Administrators	Assign system user's role	• Click on "System users" link • Click on the "Detail" button • Click on the combo box • Select an item in the combo box • Click "Add right" button	• List of System users • Information details of each System users • List of rights for System users
Administrators	Disable system user	• Click on "System users" link • Click "Toggle Status"	• List of System users • Status of System users (individually)
Administrators	Delete system user	• Click on "System users" link • Click "Delete" button	• List of System users
Administrators	Change system user password	• Click on "System users" link • Click "Change" button • Key in new password • Key in new password for verification	• List of System users • Password (New)
Administrators	Create system group	• Click on "System group" link • Click "Create New Group" button • Type group name in text box • Click "Create" button	• List of System group • System group (New)
Administrators	Assign rights to user group	• Click on "System group" link • Click combo box to select a right	• List of System group • List of rights for System groups

Subject	Object	Operations	Information
		• Click “Add rights”	
Administrators	Assign user to group	• Click on “System group” • Click combo box to select a user • Click “Add user”	• List of System group • List of System users
Administrators	Remove rights to user group	• Click on “System group” link • Click “Remove” button under “Module rights assigned to group” table	• List of System group • List of rights for System groups
Administrators	Remove user from group	• Click on “System group” link • Click “Remove” button under “Users assigned to group” table.	• List of System group • List of System users
Administrators	Search user	• Click “System user” link • Key in username in the search box • Press the “Search” button.	• List of System users
Administrators	Search group	• Click on “System group” link • Key in username in the search box • Press the “Search” button.	• List of System group
Administrators	Configure password policy	• Click “password policy” link • Set minimum password length • Set password complexity, either Alphanumeric or Alphanumeric with symbols. • Set maximum attempt	• List of password policy and options for password policy.
Administrators	Set session timeout duration	• Key in number of minutes before session time out in the text box • Set whether to allow multiple logins • Press the “Update”	• Session parameter (minutes)

Subject	Object	Operations	Information
		button	
Administrators	Add authentication server	• Click "ePassport Suite server" link • Key in server IP in the text box • Key in server port in the text box • Click "Register server"	• Server IP address • Server Port Address
Administrators	Delete authentication server	• Click "ePassport Suite server" link • Click "Remove" button	• Server IP address
Administrators	Backup ePassport Suite configuration	• Click "Backup restore" link • Click "Backup configuration" button • Select location to save the backup	• Information to create backup such as configuration file.
Administrators	Backup log files	• Click "Backup restore" link • Click "Backup log files" button • Select location to save the backup	• Information to create backup such as configuration file.
Administrators	Backup logs and clean local copy	• Click "Backup restore" link • Click "Backup & clean log files" button • Select location to save the backup	• Information to create backup such as logs
Administrators	Restore configuration	• Click "Backup restore" link • Click "Browse…" button • Locate configuration file • Press the "Restore" button.	• Information to create backup such as configuration file.
Administrators	Monitor system logs	• Click "System logs" link • View latest logs • Press "Next" to view previous logs	• List of logs and details log information.
Administrators	Filter logs	• Click "System logs" link • Enter username • Enter log duration	• List of logs and details log information.

Subject	Object	Operations	Information
		• Check either of the following check boxes: o Failure o Information o Success o Error • Press the search button	
Administrators	Export system logs in PDF	• Click “System logs” link • Apply filters to the logs • Specify number of pages in the text box • Press the “Generate PDF” button	• List of logs and details log information.
Administrators	Export system logs in CSV	• Click “System logs” link • Apply filters to the logs • Specify number of pages in the text box • Press the “Generate CSV” button	• List of logs and details log information.
Administrators	Add token user	• Click “Token users” link • Click “Crete new user” button • Type “username” and “password” • Press the “Create” button.	• List if Token users • Username
Administrators	Add authenticatio n method for token user	• Click “Token users” link • Click “Details” on a particular token users • Click combo box to select authentication type • Click the “Add” button • For OTP, Administrators must key in Token 1 and 2. • Then press the “Add” button.	• List if Token users • Creadential of Token users • OTP Token information
Administrators	Remove authenticatio	• Click “Token users” link	• List if Token users

Subject	Object	Operations	Information
	n method for token user	• Click “Details” on a particular token users • Click “Remove” from Tokens Assigned to Users list.	• Creadential of Token users
Administrators	Disable token user	• Click “Token users” link • Click “Details” on a particular token user. • Click “Toggle Status”	• List if Token users • Creadential of Token users • Info on Token users status
Administrators	Disable token for a particular user	• Click “Token users” link • Click “Details” on a particular token user. • Click “Toggle” button on a particular authentication type.	• List if Token users • Creadential of Token users • Info on Token Token status
Administrators	Remove token user	• Click “Token users” link • Click “Delete” button on a particular user. • Click “Delete” button.	• List if Token users • Information on Token
Administrators	View detail authenticatio n information on a token user	• Click “Token users” link • Click “Details” on a particular token user. • Click “Details” on a particular authentication type.	• List if Token users • Information on Token
Administrators	Search token user	• Click “Token users” link • Type token user’s username on the search box • Press the “Search” button.	• List if Token users • Information on Token
Administrators	Configure token user’s password policy	• Click “password policy” link • Set minimum password length • Set password complexity, either Alphanumeric or Alphanumeric with symbols. • Set maximum attempt	• List if Token users • Information on Token • Password

Subject	Object	Operations	Information
Administrators	Configure one time password	• Click “Mobile token” button • Configure one time password variance • Configure one time password synchronization	• List if Token users • Information on OTP (Token) details
Administrators	Monitor token logs	• Click “Token logs” link • View latest logs • Press “Next” to view previous logs	• List of logs related to OTP tokens
Administrators	Filter token logs	• Click “Token logs” link • Enter username • Enter log duration • Check either of the following check boxes: o Failure o Success • Press the search button	• List of logs related to OTP tokens • Username • Information on time
Administrators	Export token logs in PDF	• Click “Token logs” link • Apply filters to the logs • Specify number of pages in the text box • Press the “Generate PDF” button	• List of logs related to OTP tokens • Username • Information on time
Administrators	Export token logs in CSV	• Click “Token logs” link • Apply filters to the logs • Specify number of pages in the text box • Press the “Generate CSV” button	• List of logs related to OTP tokens • Username • Information on time
Administrators	Change administrator’s password	• Click “Change password” • Key in old password • Key in new password • Key in new password for confirmation • Press the “Update” button	• Old password • New password

Subject	Object	Operations	Information
Administrators	Generate system capacity report in PDF	• Click "System capacity" link • Click OTP server's IP address • Configure report time range • Click on the "Generate PDF" button	• System Capacity report in Portable Document Format (PDF)
Administrators	Generate summary report in PDF	• Click "Summary" link • Press the "Generate PDF" button	• Summary report in Portable Document Format (PDF)
Administrators	Generate detail user usage report in PDF	• Click "Detail user usage" link • Search user by key in user's username, and press the search button • Press the "Detail" button. • Press "Generate PDF" button	• Detailed User Usage report in Portable Document Format (PDF)
Administrators	Generate system capacity report in CSV	• Click "System capacity" link • Click OTP server's IP address • Configure report time range • Click on the "Generate CSV" button	• System capacity report in Comma-Saperated values file (CSV)
Administrators	Generate summary report in CSV	• Click "Summary" link • Press the "Generate CSV" button	• Summary report in Comma-Saperated values file (CSV)
Administrators	Generate detail user usage report in CSV	• Click "Detail user usage" link • Search user by key in user's username, and press the search button • Press the "Detail" button. • Press "Generate	• Detailed user usage report in Comma-Saperated values file (CSV)

Subject	Object	Operations	Information
		CSV" button	
Token user	Register token	• Launch mobile OTP software • Key in Token 1 and 2 in registration form • Key in Confirmation key on mobile phone • Press confirm	• Token 1 value • Token 2 value
Token user	Seek OTP authentication	• Launch mobile OTP software • Key in OTP number in the form • Press the submit button	• One-Time Password number

Table 10 Scope of Information Flow

The security attributes of a user has been given by TOE according to the user's group. However the Administrators have the right to modify these security attributes.

The Administrators can also delete or disable a user with the interface in the Management Console. The whole list of management functions which the TOE provides to the authorized users are listed in section 4.2.5.5.

The Administrators can assign security roles and can edit or modify access rights for the user by the user management module.

Access rights "system_configs view" and "system_logs view" allow administrators to query and view the system logs and configuration files as well as adding and modifying new system users and system groups.

The user sessions can be automatically enforced to an idle state if the account is inactive within an administrative configured duration. The time interval is between 1 minute to 30 minutes, where are the administrator configured according to the preference.

If the Administrators allow users to log in multiple concurrent sessions TOE do not enforce any limit for the number of multiple sessions. It will be a "allow without limit" or "do not allow" choice.

TOE will allow users to control their last successful access and unsuccessful attempt right after the access to the TOE. The date and time information for those events are displayed to the user in order to control their access history.

This Security Function is providing the following functional requirements;

FTA_MCS.1, FTA_SSL.1, FTA_TAH.1 FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_SMF.1, FMT_SMR.1, FDP_IFF.1 and FDP_IFC.1

5.1.4.2 Token Management (Management Console)

Administrators of the TOE can manage the attributes of desktop machine token or mobile phone token users which can generate OTP for the supported applications. Administrators can add, delete or modify user attributes and all these information are stored in Novell eDirectory. Administrators with sufficient access rights can extract these data with invoking a service via LDAP.

This Security Function is providing the following functional requirements;

FIA_ATD.1, FIA_USB.1 and FMT_MSA.1

5.1.4.3 Server Management (Management Console)

TOE provides data exchange with other applications in the operational environment and also towards ePassport Suite server allocated at other places connected via network. These import and export operations are controlled by the TOE and conducted according to an access control policy.

TOE communicates with Novell's eDirectory which is installed to the IT Environment and import and export user data via LDAP and supports the authentication module.

Also the users with sufficient access rights can import and export log reports through audit mechanism.

All these data exchange are controlled by management console and the TOE enforce an access control policy throughout the operations.

This Security Function is providing the following functional requirements;

FDP_ACC.1, FDP_IFC.1, FDP_IFF.1, FDP_ETC.1, FDP_ITC.1

End of Document