C053 Certification Report

EzIdentity™ mSign™ (Android v2.0.0.1 & iOS v2.0.0.1) and EzIdentity™ Authentication Platform v4.0.0.2

File name: ISCB-5-RPT-C053-CR-v1a
Version: v1a
Date of document: 27 December 2013
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C053 Certification Report

EzIdentity™ mSign™ (Android v2.0.0.1 & iOS v2.0.0.1) and EzIdentity™ Authentication Platform v4.0.0.2

27 December 2013

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,

No 7 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8992 6888 □ Fax: +603 8992 6841

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C053 Certification Report – EzIdentity™ mSign™ (Android v2.0.0.1 & iOS v2.0.0.1) and EzIdentity™ Authentication Platform v4.0.0.2
DOCUMENT REFERENCE:	ISCB-5-RPT-C053-CR-v1a
ISSUE:	v1a
DATE:	27 December 2013

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

The copyright of this document, which may contain proprietary information, is the property of CyberSecurity Malaysia.

The document shall be held in safe custody.

©CYBERSECURITY MALAYSIA, 2013

Registered office:

Level 5, Sapura@Mines

No 7, Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

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 27 December 2013, 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 and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

Reproduction of this report is authorized provided the report is reproduced in its entirety.

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 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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	23 December 2013	All	Final release
v1a	27 December 2013	Page iv	Add the date of the certificate.
		Table 2, Table 3	Rewording the table label text based on feedback from Scheme Certification Committee.
		Figure 1	Rewording the figure label text based on feedback from Scheme Certification Committee.

Executive Summary

EzIdentity™ mSign™ (Android v2.0.0.1 & iOS v2.0.0.1) and EzIdentity™ Authentication Platform v4.0.0.2 (hereafter referred as mSign and EzIdentity Platform) from EZMCOM Inc. are the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

The TOE is consists of two components as follows:

a) Client side: EzIdentity™ mSign. mSign is a smartphone based application that provides users with the ability to apply digital signatures to documents and data that the users receive. The application allows for the generation of a digital signature, which can then be used to approve and sign transactions (such as internet banking, funds transfers, etc.). In addition, the application supports the generation of One Time Password (OTP) for software initialisation and challenge response code in order to unblock the blocked user.

b) Server side: EzIdentity™ Authentication Platform. EzIdentity platform supports an organisations deployment of the mSign application by providing a back-end platform to manage and control deployment and configuration. The platform assists in the transfer of transaction data to be signed between third parties and mSign users, provides user and role management, security and management functions and allows organisations to manage and configure all aspects of both the EzIdentity platform and mSign application deployment.

The scope of evaluation covers major security functions described as follows:

a) **Security Audit**: EzIdentity platform generates audit records for security events. The Administrator, Super Operator and Operator who have roles with access to the audit report module are allowed to view the audit trail.

b) **Data Protection**: User data such as device ID, user PIN and signature data that is stored within mSign application is encrypted with Triple-DES encryption to prevent from data modification and unauthorised access.

c) **Identification and Authentication**: The TOE, both mSign and EzIdentity platform, enforce user identification and authentication mechanism prior to allow user to any user action or information flow being permitted. mSign user is required to enter user PIN before permitted to perform any actions. On the EzIdentity platform, users such as Administrators, Super Operators, and Operators must be authenticated using correct combination of username and password before permitted to perform any administrative functions.

d) **Security Management**: EzIdentity platform provides a wide range of security management function for Administrators including TOE configuration, manage mSign client application, managing users, assign the information flow policy, and audit management among other routine maintenance activities.

e) **TOE Access**: TOE provides session termination based on time limitation set on user inactivity. The TOE also enforce user blocking session if the user have wrongly entered user PIN after certain number of invalid authentication attempts are made. In order to unblock the session, user is required to request Challenge Response Code which will be sent to his or her registered mobile phone or email as defined during user registration process.

f) **Cryptographic Operation**: Both mSign and EzIdentity platform provide users with functionality to digitally sign files, data and sensitive transaction (such as internet banking transfer) to provide integrity and non-repudiation. It also provides One Time Password (OTP) generation, secure transit of data between TOE components and secure storage of user data on device.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for the TOE, the security requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, 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 the TOE to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that 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 BAE Systems Detica evaluation facility (the 'Detica MySEF') and completed on 26 November 2013.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the common criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that mSign and EzIdentity platform meet their requirements. It is recommended that a potential user of mSign and EzIdentity

platform to refer to the Security Target (Ref [6]) and this Certification report prior to deciding whether to purchase 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), EzIdentity™ mSign™ (Android v2.0.0.1 & iOS v2.0.0.1) and EzIdentity™ Authentication Platform v4.0.0.2 (hereafter referred as mSign and EzIdentity platform) are:

a) the client application (mSign) install in a smartphone that provides users with the ability to apply digital signatures to documents and data that the users receive. The application allows for the generation of a digital signature, which can then be used to approve and sign transactions (such as internet banking, funds transfers, etc.). In addition, the application generates challenge response codes for users to retrieve when required.

The built-in cryptographic module allows users to digitally sign their documents and transactions. User data stored on the device is encrypted with Triple-DES and is secure from tampering or modification.

b) the server application (EzIdentity platform) that supports an organisations deployment of the mSign application by providing a back-end platform to manage and control deployment and configuration. The platform assists in the transfer of transaction data to be signed between third parties and mSign users, provides user and role management, security and management functions and allows organisations to manage and configure all aspects of both the EzIdentity platform and mSign application deployment.

EzIdentity also allows organisations to connect their mSign with existing third-party Certificate Authorities (CAs) for the generation of digital signature data, along with allowing the use of external messaging services (such as email, SMS and push notifications) to inform users.

The EzIdentity provides administrative users with full control over mSign deployments, including the generation, activation/deactivation, modification and revocation of both mSign applications and their users' associated digital signature and certificate.

2 In the context of the evaluation, the TOE is expected to provide the following major security feature:

a) **Security Audit**: EzIdentity platform generates audit records for security events. It provides several types of log such as Audit Log, Token status, Certificate Audit Log, Certificate Expiry, mSign Audit Log, and Operator Log. These logs can be viewed by Administrator, Super Operator and Operator who have been assigned with roles to access and view the audit report.

b) **Data Protection:** The TOE has the capability of protecting user data which includes device ID, user PIN and signature data stored within mSign by encrypting the data. This action can prevent from data modification and unauthorised user from accessing the TOE.

c) **Identification and Authentication**: The TOE users are identified and authenticated based on the access platform. For mSign user, the user is required to enter strong and correct user PIN before being granted access to the TOE.

d) There are three types of user on EzIdentity platform. Each user is required to be authenticated with combination of username and password before being granted access to TOE. The TOE administrator is capable to install and setting up the EzIdentity platform. The TOE administrator is also capable to create and manage user role functionality for Super Operator. Super Operator is able to create and manage user role functionality for Operators and assign them with respected administrative actions.

e) **Security Management**: The EzIdentity platform gives Administrator, Super Operator and Operator a wide range of security management functions based on user role. It deploys restriction of access level based on user management level. Administrator can configure the EzIdentity platform, mSign client application, manage users, assign the information flow policy, and audit management functionality.

f) **Cryptographic Support**: The TOE provides various cryptographic operation and key generation for specific purpose and functionality. The details of the cryptographic algorithm used can be found in section 1.4 of this document.

g) **TOE Access**: TOE is able to initiate session termination based on time limit on user inactivity, requiring the user to re-authenticate before any further actions can be performed. The TOE also enforce user blocking session if the user have wrongly entered user PIN after certain number of attempts as assigned by the administrator. User is required to request Challenge Response Code that will be sending to his or her registered mobile phone or email which given during registration process.

1.2 TOE Identification

3 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	C053
TOE Name	EzIdentity™ mSign™ and EzIdentity™ Authentication Platform
TOE Version	• EzIdentity™ mSign™ (Android v2.0.0.1 & iOS v2.0.0.1) • EzIdentity™ Authentication Platform v4.0.0.2
Security Target Title	EzIdentity™ mSign™ & EzIdentity™ Authentication Platform Security Target
Security Target Version	v1.1

Security Target Date	18 November 2013
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, September 2012, Version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2
Sponsor and Developer	EZMCOM Inc 2B-23A-3, Block 2B, Plaza Sentral, Jalan Sentral 5, 50470 Kuala Lumpur, MALAYSIA.
Evaluation Facility	Detica MySEF

1.3 Security Policy

4 In order to provide user data protection, the TOE enforces access control policy to restrict the TOE access and operation to only authorise users based on their assigned roles. The TOE users are identified and authenticated based on the access platform. For mSign user, the user is required to enter strong and correct user PIN before being granted access to the TOE.

5 There are three types of user on EzIdentity platform. Each user is required to be authenticated with combination of username and password before being granted access to TOE. The TOE administrator is capable to install and setting up the EzIdentity platform. The TOE administrator is also capable to create and manage user role functionality for Super Operator. Super Operator is able to create and manage user role functionality for Operators and assign them with respected administrative actions.

6 The details of the security policy are described in Section 5.2 and Section 6 of the ST (Ref [6]).

1.4 TOE Architecture

7 The TOE includes both logical and physical boundaries which are described in Section 1.5 of the ST (Ref [6]).

1.4.1 Logical Boundaries

8 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) **Security Audit**

EzIdentity platform generates audit records, which contain the date and time of the event, type of event, subject identity, and outcome of the event, when the following security events occurs:

i) Start-up or shutdown of the audit function,

ii) Issuance of mSign activation code to the end user,

iii) mSign application activation (certificate generation),

iv) Certificate issuance,

v) SMS notification generation,

vi) Transaction status,

vii) mSign application reset, and

viii) Issuance of mSign application unlocks code (for users who have locked their application via a number of invalid login attempts).

The Administrator, Super Operator and Operator have the capability to review these audit records via the EzIdentity web interface. Timestamps are generated for audit logs by utilising the underlying operating system.

b) **Identification and Authentication**

All users are required to perform identification and authentication prior to being granted the access to any TOE functions or interfaces.

Administrator, Super Operator and Operator users may access the EzIdentity platform by providing username and password via Web Interface. Once identified and authenticated, these users will be granted to perform any actions which have been assigned based on their role. Administrator, Super Operator and Operator users may change their passwords via the EzIdentity platform portal.

The mSign application keeps a record of a unique user ID, the user-selected PIN and the device ID. These three items provide a rigid authentication structure – users must enter their PIN to access the functionality that mSign provides, but their corresponding user and device ID must also match what EzIdentity has recorded to ensure that the user is genuine.

If a user fails to provide valid PIN after 5 attempts, the mSign application will block the user and deny any further action to be taken on the TOE. The user

needs to request Challenge Response code which will be provided by the respected Operator who has the privileges to perform this function. Once a successful Challenge Response has been provided, mSign access is restored. mSign users may change their PIN once they have been authenticated via the mSign application.

c) Cryptographic Operation

Both TOE components mSign and EzIdentity, support various type of cryptographic algorithm for specific purpose and functions.

The TOE provides the following key generation functions:

i) RSA keys of 2048 bits, generated in accordance with RSA PKCS#1.

ii) Triple-DES keys of 192 bits, generated based on RFC 2898 PKCS#5 Section 5.2.

The TOE can perform encryption and decryption (along with digital signature generation and verification) operations using the following algorithms and key sizes:

i) RSA with key sizes of 2048 bits that meets the RSA PKCS#1 standard.

ii) Triple-DES with 192 bits (no specific mode of operation) that meets FIPS-46-3 standard.

The TOE also generates One-Time Password (OTP) and challenge responses using the following algorithms and key sizes:

i) Time OTP (TOTP) and the OATH Challenge Response algorithm (OCRA) with 160 bits keys that meet the RFC 4226, RFC 6328, and RFC 6287 standards.

The mSign application makes use of these functions for the generation of one-time passwords that may be used by users for two-factor authentication. The EzIdentity platform may generate Challenge Response codes to permit Operators to unlock mSign applications that have been locked due to failed authentication attempts.

The randomness used for key generation is obtained via the mobile device built-in gyroscope. The user is directed to shake their device during initial configuration of the TOE; this movement is used to generate random data. The random value is combined with the device date and time to generate a key.

The TOE may also perform hashing and hashed message authentication via the following functions:

i) Hashing is performed via SHA-1 and SHA-256, in accordance with FIPS-180-2.

ii) Hashed message authentication is performed using HMAC SHA-1, with a message digest size of 20 bytes and key sizes of 160 bits, in accordance with the FIPS 180-3 standard.

The TOE is able to zeroise cryptographic keys and other sensitive data that are no longer required or in use. This is achieved by overwriting the keys and CSPs stored in memory.

d) **Data Protection**

mSign provides the functionality for the generation of RSA key pairs. These key pairs are combined with other data to produce digital certificate. The primary function of mSign is to provide digital signature function for the signing of transactions and other sensitive exchanges. Users are able to sign transactions to ensure non-repudiation and identity assurance when performing transactions such as financial transactions and sensitive data transfer using the digital certificate.

mSign also generates One-Time Password (OTP) that can be used for two-factor authentication. The OTP can be retrieved by users via the mSign; the user does not contribute to the generation of the OTP.

mSign makes use of the Triple-DES algorithm to encrypt device-identifying data and mSign application data stored on a user's phone. This, in tandem with the underlying mobile operating system, protects user data from misuse or accidental disclosure. SHA is utilised to take a fingerprint of the application data and container-fingerprint for integrity purposes.

EzIdentity platform communicates with mSign for the transmission of certificate requests, delivery of data to be signed and the submission of signed data. This channel is logically distinct from other channels in order to protect the data that being transmitted from modification and disclosure.

e) **Security Management**

The TOE provides the following management functions:

i) EzIdentity platform provides a suite of management function to Administrator, Super Operators, and Operators based on the privileges policy as defined by the organisation. The management roles may perform the following tasks:

- Create user with default password;
- Changing of user passwords;
- Import, export, enrolment of mSign user credentials and tokens;
- Generation of challenge response codes for locked mSign application;
- User role management;
- User access control management;
- Audit report generations;
- Operator/Super Operator management.

Administrator may create and manage the Super Operator and then the Super Operator may create and manage the Operator. The management roles may access the TOE via web portal provided by EzIdentity platform.

ii) mSign users may update their PIN via the mSign application once they have been successfully authenticated with the TOE.

f) **TOE Access**

Both EzIdentity platform and mSign implement access control and authentication measures to ensure that TOE data and functionalities are not being misused by unauthorised parties.

mSign users shall enter correct user PIN before being granted to access the TOE in order to use the digital signing, OTP or any other functionalities that mSign provides. The PIN is configured during application installation and initial configuration. The users may change their own PIN as requested. Administrator roles are unable to reset a PIN if it is forgotten.

mSign user sessions will be locked after a period of two minutes idle. Once this time threshold has been met, the TOE will return to the login screen and the user must re-enter their PIN to resume TOE access.

mSign also implements session locking and deny any further access if the users enter incorrect PIN 5 times. In order to regain access to TOE, user must request Challenge Response Code from Operator or Super Operator to generate that code for them. Then users must enter the Challenge Response Code in order to restore the TOE functionality.

For EzIdentity platform, there are 3 distinguish administrative role provided: Administrator, Super Operator and Operator. Each role has different levels of access to the functions that the TOE provides. Administrators have full access and Operators will have the least access. The functions that are available to each role are adjustable by the role above them. Administrator is responsible in setting up EzIdentity platform and configuration between EzIdentity platform and mSign. Administrator is also responsible to create user domain based on the organisation requirement. Each domain may have one or more Super Operator in charged. The interface used to access the EzIdentity platform is logically distinct and separate from other interfaces on the platform.

EzIdentity platform will log-off a user session if the session is idle after 15 minutes. The users must then re-authenticate with the TOE prior to performing any further actions upon the TOE. Depending on the configuration of the Active Directory server, EzIdentity platform users may become locked out from accessing the TOE after a set number of wrong authentication attempts.

1.4.2 Physical Boundaries

9 The TOE is a software product used for digital signing of data/file/transaction that includes the client and server components of the EzIdentity. The client component (mSign application) is designed to run on a variety of mobile hardware with the minimum mobile operating systems requirements as follows:

a) Android version 4.0

b) Apple iOS version 4.0

10 The server component(EzIdentity platform), will run on any server running a Linux-based OS (such as Red Hat or CentOS) with the following minimum hardware requirements:

a) 1 CPU Quad Core (2.0 GHz);

b) 8GB RAM;

c) 150GB HDD (RAID-1); and

d) 2x 1Gbps Network

11 All of the underlying hardware and the operating systems used by both mSign and EzIdentity are out of scope for this evaluation.

12 Figure 1 identifies the major architectural components that comprise the TOE.

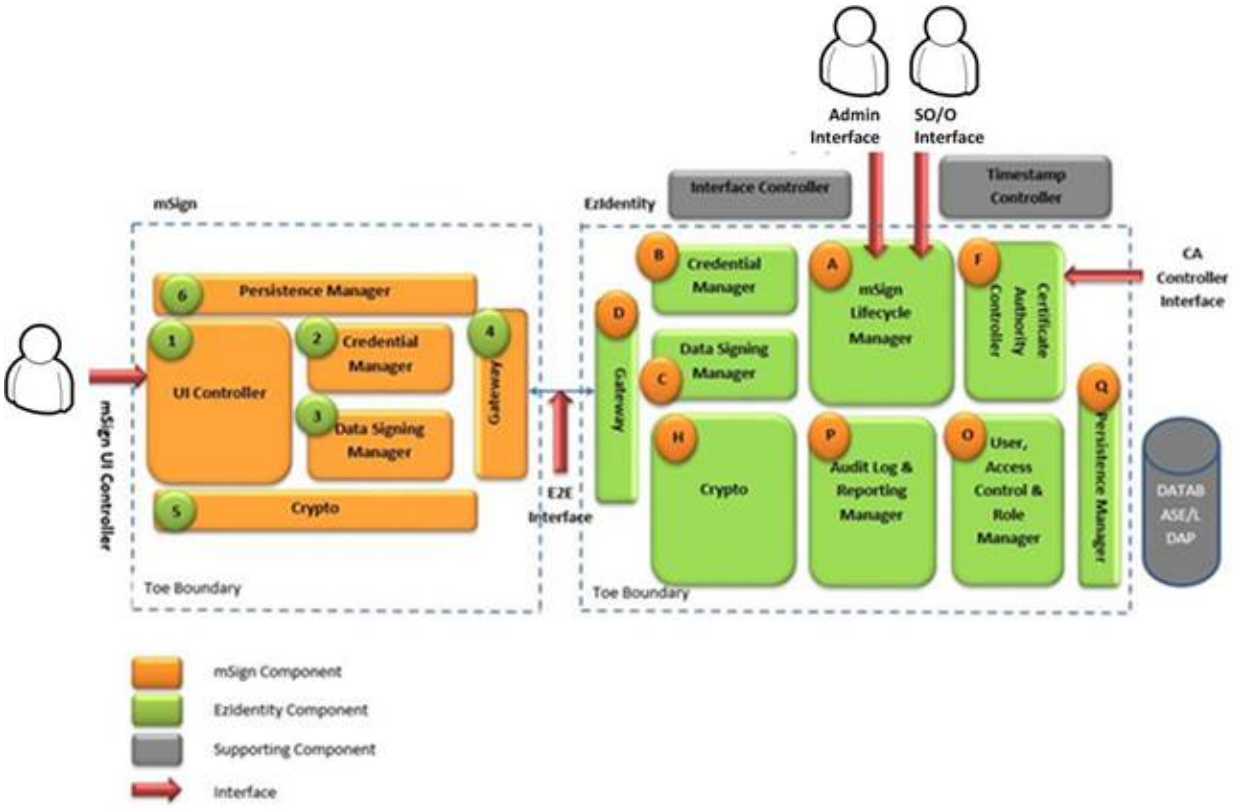

Figure 1: Architecture diagram of the TOE

13 The following Table 2 describes the components construct mSign application:

Table 2: The components of mSign application

Identifier	Subsystems	Overview
1	UI Controller	This module is responsible for providing the mSign user interface to users. It is responsible for handling all user input/output prior to processing by other subsystems of the TOE. This module takes authentication data from mSign users in the form of a numerical PIN (set during TOE

Identifier	Subsystems	Overview
		configuration) prior to permitting users to perform any action.
2	Credential Manager	This module is responsible for the initialisation and protection of mSign end-user credentials (PKI key-pairs and OTP credentials).
3	Data Signing Manager	This module receives and processes transaction files/data received from the EzIdentity platform and allows users to digitally sign them.
4	Gateway	This module is responsible for the secure data transfer and I/O between the mSign application and EzIdentity platform. It makes use of the Crypto module to secure data sent between the two platforms. The Gateway module returns transaction data and/or files.
5	Crypto	Responsible for managing all cryptographic operations performed within the mSign application.
6	Persistence Manager	This module is responsible for the secure file I/O of mSign PKI and OTP credentials between the mSign application and the underlying mobile operating system.

14 The following Table 3 describes the components construct EzIdentity platform.

Table 3: The components of EzIdentity platform

Identifier	Subsystems	Overview
A	mSign Lifecycle Manager	This module is responsible for the lifecycle management of PKI credentials for mSign users. It interfaces with the Interface Controller subsystem to receive instructions for PKI enrolment, registration, disenrollment, revocation and suspension.
B	Credential Manager	This module is responsible for the issuance and initialisation of mSign user credentials, PKI certificates and the lifecycle management of PKI/OTP credentials.
C	Data Signing	This module is responsible for processing transaction

Identifier	Subsystems	Overview
	Manager	files and data, certificate verification, digital signature verification and providing status updates to external applications regarding signature status.
D	Gateway	This module is responsible for the secure data transfer and I/O between the mSign application and EzIdentity platform. It makes use of the Crypto module to secure data sent between the two platforms. The primary function of the Gateway subsystem is to transfer transaction and file data received by the EzIdentity platform to the mSign users for review and signing. This module is also responsible for transmitting credential initialisation parameters, data to be signed by the user, push notifications and SMS notifications to the mSign.
F	Certificate Authority Controller	This module is responsible for the installation and configuration of a third-party certificate authority. It is also responsible for CSR/CRL interactions with external third-party certificate authorities.
H	Crypto	This module is responsible for managing and providing cryptographic functions to other module within the EzIdentity platform.
Q	Persistence Manager	This module is responsible for the secure I/O of mSign credentials (PKI and OTP) between the EzIdentity platform and the underlying file system (Database, LDAP)
O	User Access Control & Role Manager	This module is responsible for providing Administrators and Super Operators with the functionality to manage user store creation/association, Operator role assignment, role management, access control, and user authentication. This module also examines authentication data provided by users and provides a user interface relevant to the access control rules in place for each user.
P	Audit Log and	This module is responsible for logging auditable events and providing the functionality for

Identifier	Subsystems	Overview
	Reporting Manager	administrative users to review these event logs.

1.5 Clarification of Scope

15 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel, and secure underlying hardware and operating systems in accordance with administrator guidance that is supplied with the product.

16 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]). The TOE is a digital signature application used for signing of data/file/transaction. It consists of two components: mSign on the client side and Ezidentity platform on the server side. The list of modules constructed the TOE that is listed in Section 1.4 of this document are included in this evaluation scope. The LDAP, database, timestamp controller and interface controller are not part of the TOE scope.

17 Potential consumers of the TOE are advised that some functions and services may not have been evaluated as part of this evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

1.6 Assumptions

18 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and that required for secure operation of the TOE which is defined in subsequent sections and in the Security Target (Ref [6]).

1.6.1 Usage assumptions

19 The following is the assumption for the TOE usage:

a) The TOE administrator is not careless, wilfully negligent or hostile and complies with administrator documentation.

1.6.2 Environment assumptions

20 The following are the assumptions of the TOE environment:

a) The underlying operating system will provide reliable time stamps that will be utilised by the TOE for generating audit log timestamps.

b) The underlying operating system protects the TOE against the unauthorised access, modification or deletion of the individual TOE components that they host.

c) The TOE environment shall employ sufficient measures to ensure that all TOE data stored within the environment is protected from misuse or unauthorised access when not in use.

d) The underlying platform on which the TOE operates shall be updated with latest security patches and fixes to ensure data stored on the platform remains protected and secure.

e) The TOE server will be stored in a physical protected area that is appropriate for the information that is to be processed by the TOE.

1.7 Evaluated Configuration

21 The TOE is a software product used for digital signing of data/file/transaction that includes the client and server components of the EzIdentity. The client component, mSign, will run on any smartphone running the Android OS version 4.0 or any Apple iPhone running iOS 4.0. The server component, EzIdentity platform, will run on any server running a Linux-based OS (such as Red Hat or CentOS).

22 All of the underlying hardware and the operating systems used by both mSign and EzIdentity as described in Section 1.4.3 of the Security Target (Ref [6]) are out of scope for this evaluation.

23 The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 26d)).

1.8 Delivery Procedures

24 Based on the delivery procedure (Ref 26a)), the TOE is delivered to EZMCOM respective customers using one of the methods below:

a) Client or customer needs to complete the mSign™ Client Application MetaData Document before submit it to EZMCOM's authorised sales representative or appointed account manager. The client or customer needs to identify personnel to be designated as the Product Owner (PO) and Security Officer (SO) for the TOE in order to establish communication between EZMCOM and the respected client.

   EZMCOM will build the mSign application as per client application document received and prepared a compressed and encrypted archive of the EzIdentity platform installer and the mSign mobile application installer binaries.

   The package will be uploaded onto client designated Secure FTP (SFTP) server or EZMCOM's own SFTP server. Then, EZMCOM will securely share the password of the encrypted package with the client PO or SO. Then PO together with SO can download and decrypt the package from the server.

b) EZMCOM will deliver the bundle package of mSign client and EzIdentity platform by hand to the client designated PO or SO.

25 If any issues occur during the delivery process, the product owner and EZMCOM authorised sale representative or appointed account manager can communicate via

email, phone call or face to face to resolve the issue. It may require escalation process to respected party if any.

1.9 Documentation

26 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

27 The following guidance documentations are provided by the developer to the end user as guidance to ensure secure delivery, installation and operation of the product:

a) EZMCOM EzIdentity Lifecycle Documentation version 1.1, 20 November 2013.
b) EZMCOM EzIdentity Token Management Platform Administrator Guide (SuperOperator), version 4.0.0, 20 November 2013.
c) EZMCOM MSign User Guide, version 1.1, 21 August 2013.
d) EZMCOM EzIdentity-Installation, June 2011, version 2.1
e) EZMCOM EzIdentity™ mSign™ & EzIdentity™ Authentication Server Operator Guide, version 4.0.0, 20 November 2013.
f) EzIdentity™ mSign™ & EzIdentity™ Authentication Platform Guidance Documentation, version 1.1, 20 November 2013.

2 Evaluation

28 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). 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 the TOE, including the following components:

2.1.1 Life-cycle support

30 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

31 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of TOE during distribution to the consumer.

2.1.2 Development

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

33 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

34 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

35 The evaluators examined the TOE preparative user guidance 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

36 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from Detica MySEF at BAE Systems Detica MySEF lab, Kuala Lumpur. The detail testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

37 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

38 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

39 At EAL2, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing sample of the developer's test plan, and creating test cases that augmented the developer tests.

40 Testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The result of the independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follow:

Table 4: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
This test aims to verify that the TOE perform specification of management functions, maintain security roles, perform static attribute initialisation, perform management of TSF data and maintain user attribute definition.	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles FMT_MSA.3.1 Static attribute initialisation	• mSign UI Controller Interface • EzIdentity Administrator Interface • EzIdentity Super Operator and	**PASS**. Result as expected.

	FMT_MTD.1b Management of TSF data (EzIdentity Authentication Platform) FIA_ATD.1a User attribute definition (EzIdentity Authentication Platform)	Operator Interface	
This test aims to verify that the TOE restricts the TOE users from specifying the alternative initial values to override the default values when an object or information is created.	FMT_MSA.3.2 Static attribute initialisation	EzIdentity Administrator Interface	**PASS**. Result as expected.
This test aims to verify that the TOE restricts the ability to modify the User PIN to User (EzIdentity mSign user) and maintains User PIN and Device ID.	FMT_MTD.1a Management of TSF data (mSign) FIA_ATD.1b User attribute definition (mSign)	mSign UI Controller Interface	**PASS**. Result as expected.
This test aims to verify that the TOE detects 5 unsuccessful authentication attempts when user enter their PIN and block the usage of the TOE	FIA_AFL.1 Authentication failure handling	mSign UI Controller Interface	**PASS**. Result as expected.
This test aims to verify that the TOE enforce the access control SFP on these objects and operations: 1. User able to sign (digital signature) transaction/data 2. User able to review transaction/ data 3. User able to change/ update mSign PIN 4. User able to update	FDP_ACC.1 Subset access control	mSign UI Controller Interface	**PASS**. Result as expected.

signature 5. User able to change/ update Gateway URL/ Service Provider 6. Administrator/Super Operator able to Add/ Change/ Disable User Groups 7. Administrator able to Add/ Unassigned Super Operator 8. Super Operator able to Add/ Unassigned Operator 9. Administrator/ Super Operator/ Operator able to review Audit logs 10. EzIdentity Settings – Change/Update (Administrator) 11. Operator able to Activate/ De-Activate Token 12. Operator able to generate Token Unlock Code			
This test aims to verify that: 1. The TOE require each user to be successfully authenticated and identified before allowing any other TSF-mediated actions on behalf of that user. 2. The TOE enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: a. Users must enter a PIN before performing any action on the mSign application b. Users can update their	FDP_ACF.1 Security attribute based access control FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action FMT_MSA.1a Management of security attributes FMT_MSA.1b Management of security attributes	• mSign UI Controller Interface • EzIdentity Administrator Interface • EzIdentity Super Operator and Operator Interface	**PASS**. Result as expected.

mSign PIN once they have authenticated with the mSign application c. A user's unique device ID will be stored on the EzIdentity along with the associated User ID. d. When signing a transaction or data, a user's digital signature will be sent to the EzIdentity for verification e. User ID and passwords will be stored for all Administrators, Super Operators and Operators. f. Operators may generate Challenge Response codes to unlock a user's unlocked mSign application. g. The TOE explicitly authorise and deny access of subjects to objects 3. The TOE enforce the access control SFP to restrict the ability to change/modify the security attributes which are PIN enforcement, event or time based token and the token modules CR/SIGNATURE OTP) to Administrators, Super Operator and Operator.			
This test aims to verify that the TOE generate and perform RSA 2048 bits cryptographic generation and operation that meet the following RSA PKCS#1	FCS_CKM.1a Cryptographic key generation (RSA) FCS_COP.1a Cryptographic	mSign UI Controller Interface	**PASS**. Result as expected.

	Operation (RSA)		
This test aims to verify that: 1. The TOE generates and perform TDES 192 bit cryptographic keys that meet the following RFC 2898 PKCS#5 Section 5.2 standard 2. The TOE overwrites the cryptographic keys.	FCS_COP.1b Cryptographic Operation (TDES) FCS_CKM.1b Cryptographic key generation (TDES) FCS_CKM.4 Cryptographic key destruction	• mSign UI Controller Interface • mSign Device Interface • EzIdentity Super Operator and Operator Interface	**PASS**. Result as expected.
This test aims to verify that the TOE performs SHA-1 and SHA-256 hashing that meets the following FIPS 180-2 standard.	FCS_COP.1c Cryptographic Operation (SHA)	mSign Device Interface	**PASS**. Result as expected.
This test aims to verify that the TOE performs OTP generation, challenge response generation in accordance with a specified cryptographic algorithm (Time OTP (TOTP), OATH Challenge-Response Algorithm (OCRA)), cryptographic key sizes 160 bits RFC 4226, RFC 6328 , RFC 6287	FCS_COP.1d Cryptographic Operation (OTP)	mSign UI Controller Interface	**PASS**. Result as expected.
This test aims to verify that the TOE performs HMAC SHA-1 160 bits, message digest sizes 20 bytes keyed hash message authentication	FCS_COP.1e Cryptographic Operation (HMAC)	mSign Device Interface	**PASS**. Result as expected.
This test aims to verify that the TOE protects TSF data from disclosure/modification when it is transmitted between separate parts of the TOE.	FPT_ITT.1 Basic internal TSF data transfer protection	End-to-End Encryption Manager (E2E)	**PASS**. Result as expected.

This test aims to verify that: 1. The TOE generates and records an audit report of the following auditable events: a. Start-up and shutdown of the audit functions b. Issuance of an mSign activation code to an end user c. mSign application activation (certificate generation) d. Certificate issuance e. SMS notification generation f. Transaction status g. mSign application reset h. Issuance of an mSign application unlocks code (for users who have locked their application via a number of invalid login attempts). i. Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event 2. The TOE provides administrator, super operator and operator with the capability to read basic information from the audit records. 3. The TOE provides the audit records in a manner suitable for the user to	FAU_GEN.1 Audit data generation FAU_SAR.1 Security Audit Review	• mSign UI Controller Interface • EzIdentity Administrator Interface • EzIdentity Super Operator and Operator Interface • CA Controller Interface	PASS. Result as expected.

interpret the information.			
This test aims to verify that: 1. The TOE generates evidence of origin for transmitted certificates at the request of the recipient 2. The TOE able to relate the client ID, public key, signature algorithms of the originator of the information and the certificate serial ID, sequence identifier, identifier ID, client ID, public key, signature algorithm of the information to which the evidence applies. 3. The TOE provides a capability to verify the evidence of origin of information to recipients given that the information is digitally signed or protected.	FCO_NRO.1.1 Selective proof of origin FCO_NRO.1.2 Selective proof of origin FCO_NRO.1.3 Selective proof of origin	mSign UI Controller Interface	**PASS**. Result as expected.
This test aims to verify that: 1. The TOE lock an interactive session after 2 minutes 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. 2. The TOE require users to re-enters their PIN prior to	FTA_SSL.1 TSF-initiated session locking (mSign)	mSign UI Controller Interface	**PASS**. Result as expected.

unlocking the session			

41 All testing performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.3 Penetration Testing

42 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, functional specification, TOE design and security architecture description.

43 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialised expertise);

c) Knowledge of the TOE design and operation;

d) Window of opportunity; and

e) IT hardware/software or other requirement required for exploitation.

44 The penetration tests focused on:

a) SQL Injection;

b) Cross Site Scripting;

c) Directory Traversal;

d) Cross-site Request Forgery;

e) Security misconfiguration;

f) Failure to restrict URL Access;

g) Information Disclosure;

h) Unauthenticated access to an administrative Java Servlet;

i) Sensitive Information disclosure from the remote LDAP server;

j) Buffer overflows;

k) Data Leakage.

45 The results of the penetration testing note that there is no residual vulnerabilities found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment as specified in Section 1.4.3 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

46 Tests conducted for the TOE produced the expected results and demonstrated that the product behaved as specified in its Security Target and its functional specification.

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

3 Result of the Evaluation

48 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 EzIdentity™ mSign™ (Android v2.0.0.1 & iOS v2.0.0.1) and EzIdentity™ Authentication Platform v4.0.0.2 performed by Detica MySEF.

49 Detica MySEF found that EzIdentity™ mSign™ (Android v2.0.0.1 & iOS v2.0.0.1) and EzIdentity™ Authentication Platform v4.0.0.2 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 2 (EAL2).

50 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

51 EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

52 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

53 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

3.2 Recommendation

54 In addition to ensure secure usage of the product, below are additional recommendations for mSign and EzIdentity platform users:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable with the stated security objectives for the operational environment and it is suitably addressed.

b) The administrators and users of the TOE should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

c) The underlying operating system, database and active directory servers are patched and hardened to protect against known vulnerabilities and security configuration issues.

d) It is advice to change default password of supporting software or application which integrated with the TOE.

e) The smart phone that being used is not jailbroken and it also has deployed minimal security measurements to ensure its secure state.

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 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] EZMCOM EzIdentity™ mSign™ & EzIdentity™ Authentication Platform Security Target, version 1.1, 18 November 2013.

[7] Evaluation Technical Report – EZMCOM EzIdentity™ mSign™ & EzIdentity™ Authentication Platform, version 1.1, 26 November 2013.

A.2 Terminology

Acronyms

Table 5: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CA	Certificate Authority
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards.
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface

A.2.1 Glossary of Terms

Table 6: 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
Certifier	The certifier responsible for managing a specific certification task.
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Digital Certificate	An electronic document that uses a digital signature to bind a public key with an identity. Information such as the name of person, or organization, their address, and more. The certificate can be used to verify that a public key belongs to an individual.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65

Term	Definition and Source
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
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.
Password	A secret numeric password shared between a user and a system that can be used to authenticate the user to the system.
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.
TSF data	Data created by and for the TOE that might affect the operation of the TOE.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	The data persistently stored as files in a secure manner by the TOE.
Zeroization	A method of erasing electronically stored data or cryptographic keys by altering or deleting the contents of the data storage to prevent recovery of the data.

--- END OF DOCUMENT ---