EzIdentity™ mSign™ & EzIdentity™ Authentication platform Security Target

Common Criteria: EAL2

Version 1.1

18-NOV-13

Document management

Document identification

Document ID	EZM_EAL2_ST
Document title	EzIdentity™ mSign™ & EzIdentity™ Authentication Platform Security Target
Document date/version	1.1, 18-NOV-13

Document history

Version	Date	Description
0.1	11-JULY-13	Released for internal review.
0.2	18-JULY-13	Released to evaluators and MyCB.
0.3	14-AUG-13	Major Changes on Scope.
0.4	19-AUG-13	Released to evaluators.
0.5	22-AUG-13	Release to evaluators.
0.6	25-AUG-13	Released to evaluators.
0.7	27-SEPT-13	Updated to address EOR-ASE v1.0.
0.8	27-SEPT-13	Updated to address EOR-ASE v1.0 and addition SFR.
0.9	24-Oct-13	Updated to address re-released EOR-ASE.
1.0	1-NOV-13	Final Release.
1.1	18-NOV-13	Updated to address CAR-005.

Table of Contents

1 Security Target introduction (ASE_INT.1)

1.1 ST reference

ST Title	EzIdentity™ mSign™ & EzIdentity™ Authentication Platform Security Target
ST Identifier	EZM_EAL2_ST
ST Version/Date	1.1 (18-NOV-13)

1.2 TOE reference

TOE Title	**Client**: EzIdentity™ mSign™ **Server**: EzIdentity™ Authentication Platform
TOE Version	**EzIdentity™ mSign™**: • Android (v2.0.0.1) • iOS (v2.0.0.1) **EzIdentity™ Authentication Platform**: • v4.0.0.2

1.3 Document organization

This document is organized into the following major sections:

- Section 1 provides the introductory material for the ST as well as the TOE description (ASE_INT.1).
- Section 2 provides the conformance claims for the evaluation (ASE_CCL.1).
- Section 3 provides the definition of the security problem that the TOE has been designed to address (ASE_SPD.1).
- Section 4 defines the security objectives for the TOE and the environment (ASE_OBJ.2).
- Section 5 contains the security functional and assurance requirements derived from the Common Criteria, Part 2 and 3 respectively, which are in turn satisfied by the TOE and the development lifecycle (ASE_REQ.2).

- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 TOE overview

1.4.1 TOE usage and major security functions

The Target of Evaluation (TOE) is the EzIdentity™ mSign™ (referred to as **mSign**) digital signing application and supporting EzIdentity™ Authentication platform (referred to as EzIdentity).

- **mSign** is a smartphone based application that provides users with the ability to apply digital signatures to documents and data that they 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.

- **EzIdentity:** The EzIdentity™ Authentication 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 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 will 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.

The following table highlights the range of security functions and features implemented by the TOE.

Security function	Description
Security Audit	EzIdentity generates audit records for security events. The administrator, Super Operator and Operator users who have roles with access to the report module have the ability to view the audit trail.
Data Protection	User data (such as the device ID, user PIN and signature data) stored within the mSign application is encrypted to protect against unauthorised access or modification.
Identification and Authentication	All users are required to identify or authenticate with the TOE prior to any user action or information flow being permitted. When using the mSign application, the user must be authenticated with a strong PIN before performing any actions. On the EzIdentity, administrators, Super Operators and Operators must be authenticated before performing any administrative functions.
Security Management	EzIdentity provides a wide range of security management functions. Administrators can configure the TOE, mSign client application, manage users, the information flow policy, and audit among other routine maintenance activities. EzIdentity users access the TOE via a web-based portal, accessible through any supported web browser. Super Operators and Operators manage the various security functions they are provided with via the text boxes, radio buttons and drop-down menus that the interface provides.
Cryptographic Operation	mSign and EzIdentity provide users with the functionality to digitally sign files, data and sensitive transactions (such as internet banking transfers) to provide identity assurance and non-repudiation. The TOE also provides the functionality for the generation of One-Time Passwords (OTP), secure transit of data between TOE components and secure storage of user data on-device.
TOE Access	The TOE ensures that access to TOE functionality is session-based and controlled to prevent unauthorised access. mSign users may access the TOE via the graphical interface provided by the mobile application. EzIdentity users access the TOE via the browser-based control panel the TOE provides. The TOE closes sessions after a defined period of inactivity. The TOE may also block access if a defined number of invalid authentication attempts are made in succession.

1.4.2 TOE type

The TOE is categorised within the ***Products for Digital Signatures*** category as identified on the Common Criteria Portal for all Certified Products.

The TOE is split into two separate components – the mSign application and supporting EzIdentity.

mSign is a smartphone-based application that allows for the digital signing of transactions and documents. Users generate a key pair when installing the TOE – this key pair is then used to generate a signing certificate. This private key can then be used to sign and authorise sensitive transactions (such as online banking) or an exchange that requires a measure of non-repudiation. The mSign application also provides the functionality for the users to generate One-Time Passwords (OTP) as part of two-factor authentication solutions.

EzIdentity is a multi-layer, multi-factor strong authentication solution to guard against identity theft and phishing frauds. The Plug-and-Play interfaces of EzIdentity allow the authentication layers to be easily integrated by multiple applications within an organization.

The TOE is designed for a variety of Operating Systems and hardware platforms, such as Red Hat Enterprise Linux and CentOS for EzIdentity and iOS and Android for the mSign application.

1.4.3 Supporting hardware, software and/or firmware

As the TOE is a collection of related software applications and tools for real-time monitoring, there are several hardware components on which the TOE relies to operate effectively and, consequently, each component has different requirements.

The mSign application is designed to run on a variety of mobile hardware. However, the minimum Mobile operating systems requirements are as follows:

- Android 4.0; and
- Apple iOS 4.0

The hardware used for the EzIdentity will vary depending on the scale and size of deployment. However, the minimum hardware requirements are as follows:

- 1 CPU Quad Core (2.0 GHz);
- 8GB RAM;
- 150GB HDD (RAID-1); and
- 2x 1Gbps Network Ports

HSM (Safenet / Thales)The EzIdentity has the minimum software requirements:

- CentOS 5.3 (or above) or Red Hat Enterprise 5.3 (or above); and
- Mozilla Firefox

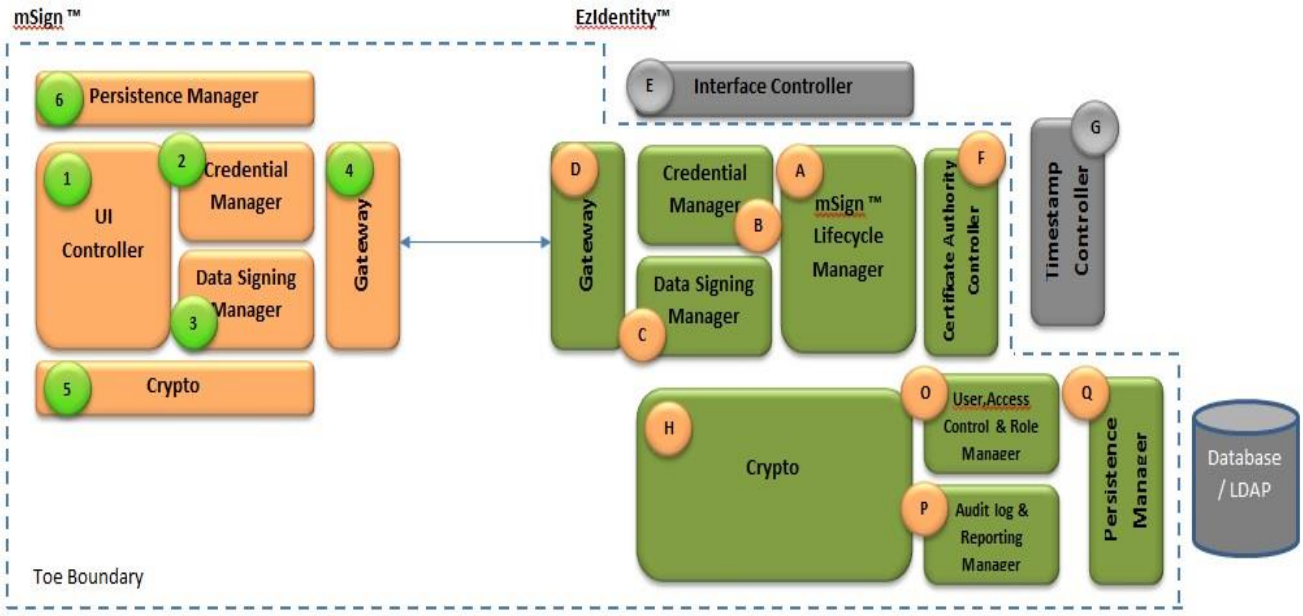
Other software pre-requisites for EzIdentity (such as sshd and OpenLDAP) are provided as part of the default installation of CentOS and Red Hat Enterprise.

1.5 TOE description

1.5.1 Physical scope of the TOE

Product Architecture

The TOE includes the client and servers components of the EzIdentity. The Client components are referred to here on as mSign.



TOE Boundary components

mSign™

Block#	Module Name	Functional Responsibility	Dependencies
1	UI Controller	This module is responsible for USER I/O. It is responsible for secure (sand boxed) display and interaction with the end user of mSign™ application User I/O – 1. Capture randomness from user 2. Display initialization progress and status 3. Get user input for initialization of PIN 4. Get user input for viewing and interaction of Data to be signed 5. Get user input for approval / rejection (Digital Signing) along with optional or mandatory Comments 6. Display data to be signed (Transaction/ File) along with its expiry time if any 7. Display notifications	Block#2, Block#3
2	Credential Manager	This module is responsible for initialization and protection of the end user mSign™ credentials: 1. Initialize (PKI) key pair 2. Initialize (OTP) Token credentials 3. Protect the PKI and OTP credentials 4. Lifecycle management of PKI and OTP credentials	Block#6, Block#5, Block#4, Block#1
3	Data Signing Manager	Receive and Process the Transaction/ File/ Data to be Digitally Signed by end user, and its expiry, include (optional) additional comments from end user	Block#6, Block#5, Block#4, Block#2, Block#1
4	Gateway	Responsible for Secure Network I/O between mSign™ app and Ezidentity™ server. End to End (tunnel) encryption is implemented using Crypto module as and when required for secure network transmission via HTTP protocol Network I/O – 1. Receive and Transmit securely Credential initialization parameters 2. Receive and Transmit Data to be Signed by user 3. Receive notifications from Ezidentity™ server	Block#5, Block#3, Block#2
5	Crypto	Responsible for all cryptographic operations required by dependent modules of mSign™ app 1. Triple DES 192-BIT 2. RSA key-pair generation 3. PBKDF2 for key derivation 4. RSA PKCS#1 V2.1 5. HOTP 6. TOTP 7. OCRA 8. SHA-1 9. HMAC-SHA1	None
6	Persistence Manager	Responsible for secure FILE I/O (Persistence) of mSign™ Credentials (PKI and OTP) to the mobile device file system	Block#5

Ezidentity™

Block#	Module Name	Functional Responsibility	Dependencies
		mSign™ components	
A	mSign™ Lifecycle Manager	This module is responsible for lifecycle management of the mSign™ PKI credentials of end users. It interacts with the Interface controller to receive message based instructions from integrating applications or the Ezidentity™ (web) Portal for:	Block#E, Block#H

		1. Enrollment (of end user for mSign™ capabilities in an integrating application) 2. Registration (of end user mSign™ credentials with an integrating application) 3. Disenrollment (of mSign™ end user in an integrating application) 4. Revocation (of mSign™ end user credentials) 5. Suspension/ Reactivation (of mSign™ end user credentials)	
B	Credential Manager	This module is responsible for initialization and protection of the end user mSign™ credentials: 1. Issue activation code 2. Initialize PKI and OTP Token credentials 3. Issue self-signed or obtain Certificate Authority X509v3 (PKI) Certificate 4. Lifecycle management of PKI and OTP credentials	Block#A, Block#D, Block#F, Block#H
C	Data Signing Manager	1. Receive and Process the Transaction/ File/ Data to be Digitally Signed by end user from mSign™ app, and its expiry 2. Verify Certificate validity, Expiry, Revocation status 3. Receive and Process the Digitally Signed Transaction/ File/ Data from mSign™ app and verify the Digital Signature 4. Callback/ Provide integrating applications on status of Digitally Signed Transaction/ Data/ File	Block#B, Block#D, Block#E, Block#F, (Block#G)
D	Gateway	Responsible for Secure Network I/O between mSign™ app and Ezidentity™ server. End to End (tunnel) encryption is implemented using Crypto module as and when required for secure network transmission via HTTP protocol Network I/O – 1. Receive and Transmit securely Credential initialization parameters 2. Receive and Transmit Data to be Signed by user 3. Send Push notifications from Ezidentity™ server 4. Send SMS notifications from Ezidentity™ server	Block#B, Block#C, Block#H
F	Certificate Authority Controller	1. Installation and configuration of external (3rd Party) Certificate Authority 2. Responsible for CSR, CRL interaction with an external (3rd Party) Certificate Authority	Block#B, Block#H
		Ezidentity™ common	
H	Crypto	Responsible for all cryptographic operations required by dependent modules of mSign™ and EzToken™ 1. Triple DES 192-BIT	None

		2. RSA key-pair generation 3. PBKDF2 4. RSA PKCS#1 v2.1 5. HOTP 6. TOTP 7. OCRA 8. SHA-1 9. HMAC-SHA1	
Q	Persistence Manager	Responsible for secure FILE I/O (Persistence) of mSign™, EzToken™ Credentials (PKI and OTP) to the file system (Database, LDAP)	Block#H
O	User Access Control and Role Manager	Responsible for – 1. User store creation/ association 2. Assignment of Operator users 3. Role management 4. Access Control 5. User authentication	Block#E
P	Audit log and Reporting Manager	Audit logging, Report generation	Block#E

1.5.2 Logical scope of the TOE

The logical boundary consists of the security functionality of TOE is summarized below.

- **Security Audit:** The server-side TOE component (**EzIdentity**) generates audit records for security events. The administrator and Operator users who have roles with access to the report module have the ability to view the audit trail.

- **Identification and Authentication:** All users are required to perform identification and authentication with the TOE before any information flows are permitted. On the server side TOE (**EzIdentity**), Administrators, Super Operators and Operators must be authenticated prior to performing any administrative functions. Depending on the configuration and policy

of the LDAP (Microsoft Active directory) that the EzIdentity is configured with, multiple incorrect attempts to authenticate with the TOE will LOCK the user account.

When using the client side application (**mSign**) the user must authenticate with the TOE (via PIN entry) before performing any authentication or authorization functions within the TOE. After 5 failed authentication attempts, user access to the token will be blocked. The TOE will then delete all sensitive data stored and re-initialize itself.

- **Cryptographic Operation:** The TOE provides a cryptographic library that utilizes the following cryptographic algorithms/functions:
    - Triple-DES (192-bit keys)
    - RSA PKCS#1 v2.1
    - OATH TOTP
    - OCRA
    - SHA-1
    - SHA-256
    - HMAC-SHA1; and
    - PBKDF2

- **Security Management:** The TOE maintains role-based access control mechanisms to ensure that functions are restricted to those who have the privilege to access them. The administrator has the ability to create Super Operators, who have privileged access to all functions related to Token management and can create Operator-class users with specific roles. The administrator Super Operators and Operators can configure the client side application for various security functionalities.

- **TOE Access:** User sessions are controlled by the TOE and both mSign and EzIdentity sessions are terminated after a defined period of inactivity, requiring the user to re-authenticate with the TOE before any further actions can be performed. Users may also be denied access to the TOE if a number of invalid authentication attempts are made. If this occurs, a system administrator must provide the user with an unlock code in order to restore access to the TOE.
- **Data Protection:** The TOE utilizes the built-in cryptographic engine to ensure that user data is protected and integrity is maintained, allowing users to remain confident in the security of transactions performed using the TOE or of any sensitive personal data that Is stored within the mSign application.

Please note that the RSA encryption and decryption operations performed on the EzIdentity are out of scope for this evaluation.

2 Conformance Claim (ASE_CCL.1)

The ST and TOE are conformant to version **3.1 (REV 4)** of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- **Part 2 conformant.** Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 4), September 2012
- **Part 3 conformant, EAL2.** Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1 (REV 4). Evaluation is EAL2, September 2012.

3 Security problem definition (ASE_SPD.1)

3.1 Overview

This section describes the nature of the security problem that the TOE is designed to address. The security problem is described through:

a) a series of ***threats*** that the TOE has been designed to mitigate,

b) specific ***assumptions*** about the security aspects of the environment (both IT related and non-IT related elements) in which the TOE will operate, and

c) any relevant ***organisational security policies*** are any statements made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

Identifier	Threat statement
T.COMINT	An unauthorised user may attempt to compromise the integrity of the data collected, processed and transmitted by the TOE by bypassing a security mechanism.
T.MODIFY	An unauthorised user may attempt to modify the TOE memory to compromise the confidentiality or integrity of the protected resources on the TOE.
T.TSFDATA	An attacker may compromise the confidentiality and/or integrity of TSF data by monitoring and/or attempting to actively modify communications between the mSign and EzIdentity.
T.UNAUTHORISED_ACCESS	A user may gain unauthorized access to the TOE and residing data.

3.3 Organisational security policies

No organisational security policies have been defined regarding the use of the TOE.

3.4 Assumptions

Identifier	Assumption statement
A.ADMIN	The Administrator is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.
A.OS	The operating systems supporting the TOE components protect against the unauthorized access, modification or deletion of the individual TOE components that they host.
A.TIMESTAMP	The underlying operating system will have a reliable time source that the TOE can utilize for generating audit log timestamps.
A.DATACONTROL	The underlying 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.
A.UPDATE	The underlying platform on which the TOE operates will be regularly updated with the latest security patches and fixes to ensure data stored on the platform remains protected and secure.
A.PHYSICAL	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.

4 Security objectives (ASE_OBJ.2)

4.1 Overview

The security objectives are a concise statement of the intended response to the security problem defined in Section 3. There are security objectives for the TOE to address and additional objectives that provide specific direction for the intended in environment in which the TOE is to operate.

4.2 Security objectives for the TOE

Identifier	Objective statements
O.CRYPT	The TOE implements cryptographic functions (HMAC SHA-1, OATH TOTP, TDES, SHA-1, SHA-256, OCRA, PKCS#1 v2.1, PBKDF2) compliant to the relevant industry standards.
O.COMMSEC	The TOE shall utilize end to end tunnel encryption using cryptographic module to ensure that sensitive data sent between the EzIdentity and mSign platforms is secured and protected from tampering or modification.
O.MODIFY	The TOE shall ensure that the protected resources stored in memories are protected against unauthorised modification.
O.CONTROL	The TOE shall restrict TOE security and management functions to authorised roles.
O.KEYPROTECT	O.KEYPROTECT shall ensures that all cryptographic keys stored within the TOE are protect sufficiently to prevent their disclosure to a malicious entity.

4.3 Security objectives for the environment

Identifier	Objective statements
OE.INSTALL	The TOE shall be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures.
OE.ADMIN	The administrator assigned to oversee the EzIdentity is trusted by the organisation and are trained in use of the TOE.
OE.OPSYS	The operating system on the underlying platform shall meet the minimum requirements for the TOE and shall be updated prior to installation to provide underlying security to the TOE.

Identifier	Objective statements
OE.ENVIRONMENT	The sites of the TOE server are physically secure sites. The physical and logical access control process is well documented with proper configuration and change management systems. The staffs at these sites are well-trained to handle the TOE securely.
OE.UPDATE	The developer shall provide updates of the TOE on a regular basis.
OE.TIMESTAMP	The platform on which the TOE is installed shall have a reliable time source (ideally set via the internet using reliable sources, such as NIST) for the generation of timestamps for audit purposes.

4.4 TOE security objectives rationale

The following table demonstrates that all security objectives for the TOE trace back to the threats and OSPs in the security problem definition.

Threats/OSPs	Objectives	Rationale
T.COMINT	O.CRYPT O.KEYPROTECT	T.COMINT concerns the integrity of the data collected processed and transmitted between TOE components and the risk of this data being modified by an attacker by bypassing the security mechanism. O.CRYPT will ensure that the data collected and transmitted by TOE using cryptographic algorithms is done so in compliance to standards and protected from attacks that attempt to bypass the security mechanisms of TOE. O.KEYPROTECT ensures that all cryptographic keys stored within the TOE are protected sufficiently to prevent their disclosure to a malicious entity.

T.MODIFY	O.MODIFY	T.MODIFY concerns any users that may try to performed unauthorised modifications to the TOE data stored in memory, in an attempt to compromise the confidentiality or integrity of TOE data and resources. This may include the unauthorised loading of software onto the TOE. O.MODIFY ensures that any TOE resources loaded into or stored in memory are adequately protected against modification or unauthorised access.
T.TSFDATA	O.COMMSEC	T.TSFDATA concerns a potential Man-in-the-Middle scenario, whereby a malicious third party attempts to intercept, modify and misuse TOE data. O.COMMSEC ensures that data sent between the two TOE components is secure and protected from modification or tampering.
T.UNAUTHORISED_ACCESS	O.CONTROL	T.UNAUTHORISED_ACCESS concerns an unknown or unauthorised user gaining access to the TOE, its functions, or its data. O.-CONTROL ensures that there is a robust access control system in place to restrict TOE data and management functions to authorised users only.

4.5 Environment security objectives rationale

The following table demonstrates that all security objectives for the operational environment all trace back to assumptions or OSPs in the security problem definition.

Assumptions	Objectives	Rationale
A.ADMIN	OE.ADMIN	This security objective has been established to directly address this assumption.
A.TIMESTAMP	OE.TIMESTAMP	This security objective has been established to directly address this assumption.
A.PHYSICAL	OE.ENVIRONMENT	This security objective has been established to directly address this assumption.
A.UPDATE	OE.UPDATE	This security objective has been established to directly address this assumption.

A.OS	OE.OPSYS	This security objective has been established to directly address this assumption.
A.DATACONTROL	OE.ENVIRONMENT	This security objective has been established to directly address this assumption.

5 Derived security requirements (ASE_REQ.2)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 4) of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a letter at the end of the component identifier as follows FDP_IFF.1a and FDP_IFF.1b.

5.2 Security functional requirements

5.2.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.1 above and itemised in the table below.

Identifier	Title
FAU_GEN.1	Audit data generation
FAU_SAR.1	Audit review
FCO_NRO.1	Selective proof of origin
FCS_CKM.1a	Cryptographic key generation (RSA)
FCS_CKM.1b	Cryptographic key generation (TDES)
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1a	Cryptographic Operation (RSA)
FCS_COP.1b	Cryptographic Operation (TDES)
FCS_COP.1c	Cryptographic Operation (SHA)
FCS_COP.1d	Cryptographic Operation (OTP)
FCS_COP.1e	Cryptographic Operation (HMAC)
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FIA_AFL.1	Authentication failure handling
FIA_ATD.1a	User attribute definition (EzIdentity)
FIA_ATD.1b	User attribute definition (mSign)
FIA_UID.2	User identification before any action
FIA_UAU.2	User authentication before any action
FMT_MSA.1a	Management of security attributes (Administrator)
FMT_MSA.1b	Management of security attributes (Operator/Super Operator)
FMT_MSA.3	Static attribute initialisation

Identifier	Title
FMT_MTD.1a	Management of TSF data (mSign)
FMT_MTD.1b	Management of TSF data (mSign)
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_ITT.1	Basic internal TSF data transfer protection
FTA_SSL.1	TSF-initiated session locking (mSign)

5.2.2 FAU_GEN.1 Audit data generation

Hierarchical to:	No other components.
FAU.GEN.1.1	The TSF shall be able to generate an audit report of the following auditable events: a) Start-up and shutdown of the audit functions; b) All auditable events for the [***not specified***] level of audit; and c) [**Specifically defined auditable events listed below**].
FAU.GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**none**].
Dependencies:	FPT.STM.1 Reliable time stamps
Notes:	Auditable events within the TOE: • Issuance of an mSign activation code to an end user; • mSign application activation (certificate generation); • Certificate issuance; • SMS notification generation; • Transaction status; • mSign application reset; and Issuance of an mSign application unlocks code (for users who have locked their application via a number of invalid login attempts).

5.2.3 FAU_SAR.1 Security Audit Review

Hierarchical to:	No other components.
FAU_SAR.1.1	The TSF shall provide [**administrator, super operator and operator**] with the capability to read [**basic information**] 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.
Dependencies:	FAU_GEN.1 Audit data generation
Notes:	None.

5.2.4 FCO_NRO.1 Selective proof of origin

Hierarchical to:	No other components.
FCO_NRO.1.1	The TSF shall be able to generate evidence of origin for transmitted [**certificates**] at the request of the [***recipient***].
FCO_NRO.1.2	The TSF shall be 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, public key, signature algorithm**] of the information to which the evidence applies.
FCO_NRO.1.3	The TSF shall provide a capability to verify the evidence of origin of information to [***recipient***] given [**that the information is digitally signed or protected**].
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.5 FCS_CKM.1a Cryptographic key generation (RSA)

Hierarchical to:	No other components.
FCS_CKM.1a.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**RSA key generation**] and specified cryptographic key sizes [**2048 bits**] that meet the following: [**RSA PKCS#1**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.6 FCS_CKM.1b Cryptographic key generation (TDES)

Hierarchical to:	No other components.
FCS_CKM.1b.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Triple-DES**] and specified cryptographic key sizes [**192 bits**] that meet the following: [**RFC 2898 PKCS#5 Section 5.2**].
Dependencies:	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.7 FCS_CKM.4 Cryptographic key destruction

Hierarchical to:	No other components.
FCS_CKM.4.1	The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method: [**overwrite the keys**] that meets the following: [**no standard**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]
Notes:	None.

5.2.8 FCS_COP.1a Cryptographic Operation (RSA)

Hierarchical to:	No other components.
FCS_COP.1a.1	The TSF shall perform [**RSA encryption, decryption, signing, verification**] in accordance with a specified cryptographic algorithm [**RSA**] and cryptographic key sizes [**2048 bits**] that meet the following: [**RSA PKCS#1**]**.**
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.9 FCS_COP.1b Cryptographic Operation (TDES)

Hierarchical to:	No other components.
FCS_COP.1b.1	The TSF shall perform [**TDES encryption and decryption**] in accordance with a specified cryptographic algorithm [**Triple-DES**] and cryptographic key sizes [**192 bits for TDES keys**] that meet the following: [**FIPS 46-3**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	Implemented with PBES2 as specified in PKCS#5 and used to encrypt mSign data stored on mobile platforms.

5.2.10 FCS_COP.1c Cryptographic Operation (SHA)

Hierarchical to:	No other components.

FCS_COP.1c.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA-1, SHA-256**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.11 FCS_COP.1d Cryptographic Operation (OTP)

Hierarchical to:	No other components.
FCS_COP.1d.1	The TSF shall perform [**OTP generation, challenge response generation**] in accordance with a specified cryptographic algorithm [**Time OTP (TOTP), OATH Challenge- Response Algorithm (OCRA)]** and cryptographic key sizes [**160 bits**] that meet the following: [**RFC 4226, RFC 6328 , RFC 6287**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.12 FCS_COP.1e Cryptographic Operation (HMAC)

Hierarchical to:	No other components.
FCS_COP.1e.1	The TSF shall perform [**keyed hash message authentication**] in accordance with a specified cryptographic algorithm [**HMAC SHA-1**] and cryptographic key sizes [**160 bits, message digest sizes 20 bytes**] that meet the following: [**FIPS PUB 180-3**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	None.

5.2.13 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**access control SFP**] on [**objects listed in the table below**].
Dependencies:	FDP_ACF.1 Security attribute based access control

Notes:

Subject	Object	Operation
User	Digital Signature	Sign transaction / data
User	Digital Signature	Review transaction / data
User	mSign PIN	Change / Update
User	Signature	Update
User	Gateway URL / Service Provider	Change / Update
Administrator	User Groups	Enable / Disable
Administrator / Super Operator	Super Operator	Add / Un-assign
Administrator / Super Operator	Normal Operator	Add / Un-assign
Administrator / Super Operator/ Operator	Audit logs	Review
Administrator	Settings	Change / Update
Operator	Token	Activate / De-Activate
Operator	Token Unlock Code	Generate

5.2.14 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**access control SFP**] to objects based on the following: [**as listed in the Notes section of FDP_ACC.1**].
FDP_ACF.1.2	The TSF shall 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 mSign PIN once they have authenticated with the mSign application** **c) User's unique device ID will be stored on the EzIdentity.** **d) When signing a transaction, 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.]
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**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.2.15 FIA_AFL.1 Authentication failure handling

Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [***[*5*]***] unsuccessful authentication attempts occur related to [**user entering their passphrase (PIN) for authentication to the TOE**].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**block usage of the TOE**].
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	None.

5.2.16 FIA_ATD.1a User attribute definition (EzIdentity)

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**Username, Password, Role**]
Dependencies:	No dependencies.
Notes:	None.

5.2.17 FIA_ATD.1b User attribute definition (mSign)

Hierarchical to:	No other components.
FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual users: [**User PIN, Device ID**]
Dependencies:	No dependencies.

Notes:	None.

5.2.18 FIA_UAU.2 User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
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.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.19 FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
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.
Dependencies:	No dependencies
Notes:	None.

5.2.20 FMT_MSA.1a Management of security attributes (Administrator)

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**access control SFP**] to restrict the ability to [***change_default, modify]*** the security attributes [**pin enforcement, event or time based token and the token modules (CR/SIGNATURE OTP)**] to [**Administrators**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	**Challenge-Response, CR** A value is provided by the EzIdentity for which the mSign will use to generate an OTP. The mSign will then pass the generated OTP to the EzIdentity for verification. **SIGNATURE OTP** The mSign chooses a value and generates an OTP based on the value. The mSign then passes both the value and the OTP to the EzIdentity for verification. In mSign, signature OTP is used when transactions/documents are signed. The user signs the hash of the document/transaction to produce a signature. An OTP is generated based on the generated signature. The user sends the OTP and the

	signature to the server.

5.2.21 FMT_MSA.1b Management of security attributes (Operator/Super Operator)

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**access control SFP**] to restrict the ability to [***change_default, modify]*** the security attributes [**time based token and the token modules (CR/SIGNATURE OTP)**] to [**Super Operator and Operator**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	**Challenge-Response, CR** A value is provided by the EzIdentity for which the mSign will use to generate an OTP. The mSign will then pass the generated OTP to the EzIdentity for verification. **SIGNATURE OTP** The mSign chooses a value and generates an OTP based on the value. The mSign then passes both the value and the OTP to the EzIdentity for verification. In mSign, signature OTP is used when transactions/documents are signed. The user signs the hash of the document/transaction to produce a signature. An OTP is generated based on the generated signature. The user sends the OTP and the signature to the server.

5.2.22 FMT_MSA.3 Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**access control SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.23 FMT_MTD.1a Management of TSF data (mSign)

Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to [***modify***] the [**User PIN**] to [**User**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.24 FMT_MTD.1b Management of TSF data (EzIdentity)

Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to [***manage***] the [**TSF data on the EzIdentity**] to [**Operators, Super Operators and Administrators**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.2.25 FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: [**a) creation of users with default passwords (mSign)** **b) changing of user passwords** **c) import, export, enrolment of mSign user** **d) generation of challenge response codes for locked mSign applications** **e) user role management** **f) user access control management** **g) audit report generation** **h) Operator/Super Operator user management**].
Dependencies:	No dependencies.
Notes:	These functions are performed via the **EzIdentity** platform only. While Administrators, Super Operators and Operators have access to this platform, the actual functionality from the above list available to each role may differ depending on how each role has been configured. See FDP_ACC.1 for more information.

5.2.26 FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**User, Administrator, Super Operator, and Operator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.2.27 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from [***disclosure, modification***] when it is transmitted between separate parts of the TOE.
Dependencies:	No dependencies.
Notes:	None.

5.2.28 FTA_SSL.1 TSF-initiated session locking (mSign)

Hierarchical to:	No other components.
FTA_SSL.1.1	The TSF shall 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.
FTA_SSL.1.2	The TSF shall require the following events to occur prior to unlocking the session: [**user re-enters their PIN**].
Dependencies:	FIA_UAU.1 Timing of authentication
Notes:	None.

5.3 TOE Security assurance requirements

EAL2 requires evidence relating to the design information and test results, but does not demand more effort on the part of the developer than is consistent with good commercial practice.

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.

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.

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

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Parts of the TOE CM coverage
	ALC_CMC.2 Use of a CM system
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample

Assurance class	Assurance components
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4 Security requirements rationale

5.4.1 Dependency rationale

Below demonstrates the mutual supportiveness of the SFR's for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE, and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level EAL2 as defined in Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
FAU.GEN.1	FPT_STM.1 Reliable time stamps	FPT_STM.1 has not been included as the TOE obtains all audit timestamps from the underlying platform. This has been addressed in Section 3.4 by A.TIMESTAMP.
FAU.SAR.1	FAU.GEN.1 Audit data generation	FAU.GEN.1
FCO_NRO.1	FIA_UID.1 Timing of identification	FIA_UID.2
FCS_COP.1a	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1a FCS_CKM.4
FCS_COP.1b	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1b FCS_CKM.4

SFR	Dependency	Inclusion
FCS_COP.1c	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	None. No keys are needed for hashing
FCS_COP.1d	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	FCS_CKM.1b FCS_CKM.4
FCS_COP.1e	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	None. No keys are needed for hashing
FCS_CKM.1a	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1a FCS_CKM.4
FCS_CKM.1b	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	FCS_COP.1d FCS_COP.1b FCS_CKM.4
FCS_CKM.4	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	FCS_CKM.1a FCS_CKM.1b
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2
FIA_ATD.1a	No dependencies	NA
FIA_ATD.1b	No dependencies	NA
FIA_UAU.2	FIA_UID.1 Timing of identification	FIA_UID.2
FIA_UID.2	No dependencies	N/A

SFR	Dependency	Inclusion
FMT_MSA.1a	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.1b	[FDP_ACC.1 Subset access control or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_SMA.1 -Management of security attributes FMT_SMR.1 Security Role	FMT_SMR.1 FMT_SMA.1
FMT_MTD.1a	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_MTD.1b	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMR.1 FMT_SMF.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2
FPT_ITT.1	No dependencies	N/A
FTA_SSL.1	FIA_UAU.1 Timing of authentication	FIA_UAU.2

5.4.2 Mapping of SFRs to security objectives for the TOE

Security objective	Mapped SFRs	Rationale
O.KEYPROTECT	FAU_GEN.1	The TOE allows set of rules to be applied to indicate authorised and unauthorised access of every user.
	FAU_SAR.1	The TOE maintain a profile of system usage and suspicion rating to each profile along with threshold condition to indicate possible security violation.
	FIA_AFL.1	The requirement helps meet the objective by blocking authentication failure after number of attempt.

Security objective	Mapped SFRs	Rationale
	FIA_UAU.2	The requirement helps meet the objective by authenticating user before any TSF mediated actions.
	FIA_ATD.1a/b	The requirement helps meet the objective by ensuring user security attributes are maintained.
	FMT_SMF.1	The requirement helps meet the objective by providing management functions of the TOE for authenticated user.
	FMT_SMR.1	The requirement helps meet the objective by providing user timing of identification.
O.CRYPT	FCS_CKM.1	Generate cryptographic keys in accordance with a specified cryptographic key generation algorithm.
	FCS_CKM.4	The requirement helps to meet the objective by destroying cryptographic keys in accordance with a specified cryptographic key destruction method.
	FCS_COP.1	Perform cryptographic operation in accordance with a specified cryptographic algorithm.
	FCO_NRO.1	The requirement allows for the use of digital signatures to provide non-repudiation.
O.MODIFY	FMT_MTD.1a	The requirement helps meet the objective by restricting the ability to modify the user password.
	FMT_MSA.1	The requirement helps to meet the objective by restricting the ability to modify the security attributes for the administrator.
O.CONTROL	FMT_MTD.1a	The requirement helps meet the objective by restricting user access to management functions.
	FMT_MTD.1b	The requirement helps meet the objective by restricting user access to management functions.
	FMT_MSA.1	The requirement helps meet the objective by restricting user access to security attributes.
	FMT_MSA.3	The requirement helps meet the objective by restricting access to provide default values for security attributes that are used to enforce the SFP.
	FMT_SMR.1	The requirement helps meet the objective by defining the security roles used within the TOE.
	FIA_AFL.1	The requirement helps meet the objective by defining limits on failed authentication attempts.

Security objective	Mapped SFRs	Rationale
	FDP_ACC.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FDP_ACF.1	The requirement provides access control functionality to ensure that access to security functionality is controlled.
	FTA_SSL.1	This requirement helps meet the objective by locking user sessions after a pre-determined period of time.
O.COMMSEC	FPT_ITT.1	The requirement ensures that data sent by users is protected from modification or disclosure.

5.4.3 Justification for SAR selection

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2).

TOE has a low to moderate level of assurance in enforcing its security functions when instantiated in its intended environment, which imposes no restrictions on assumed activity on applicable networks. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a Basic attack potential.

6 TOE summary specification (ASE_TSS.1)

6.1 Overview

This section provides the TOE summary specification, a high-level description of how the TOE actually implements the claimed security functional requirements. The TOE provides the following security functions:

- **Security Audit;**
- **Identification and Authentication;**
- **Cryptographic Operation;**
- **Data Protection;**
- **Security Management; and**
- **TOE Access**

6.2 Security Audit

EzIdentity will create audit records (which contain the data and time of the event, type of event, subject identity and outcome of the event) when the following events occur (FAU_GEN.1):

- Startup or shutdown of the audit function;
- Issuance of an mSign activation code to an end user;
- mSign application activation (certificate generation);
- Certificate issuance;
- SMS notification generation;
- Transaction status;
- mSign application reset; and
- Issuance of an mSign application unlocks code (for users who have locked their application via a number of invalid login attempts).

Operator, Super Operator and Administrator users all have the capability to review these audit records via the EzIdentity web interface (FAU_SAR.1). Timestamps are generated for audit logs by

utilising the underlying operating system. The TOE does not generate its own timestamps for use in audit records; these are supplied by the underlying operating system.

6.3 Identification and Authentication

The TOE keeps record of a number of items of user data for authentication purposes. Users must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces (other than the login interface).

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 (FIA_ATD.1a, FIA_UAU.2 and FIA_UID.2).

If a user fails to provide a valid PIN after 5 attempts, the mSign application will deny any further access until a Challenge Response is provided (FIA_AFL.1). This CR can only be obtained by an EzIdentity Operator with sufficient permissions to generate these codes. Once a successful Challenge Response has been provided, mSign access is restored. mSign users may change their PIN via the mSign application once they have authenticated (FMT_MTD.1a).

Administrator, Super Operator and Operator-role users may access the EzIdentity via the web portal that the platform provides. These roles must provide a username and password for authentication with the TOE (FIA_ATD.1b). Once the TOE verifies that the provided username and password are authentic, the user will be provided with the portal interface that provides access to the functions assigned to their user ID/role (FMT_SMR.1). Administrator/Super Operator and Operator users may change their passwords via the EzIdentity portal.

6.4 Cryptographic Operation

Both TOE components make use of a built-in cryptographic library which allows for both cryptographic key generation and cryptographic functions to be performed.

The TOE provides the following key generation functions:

- **RSA** keys of **2048** bits, generated in accordance with **RSA PKCS#1** (FCS_CKM.1a); and
- **Triple-DES** keys of **192** bits, generated in accordance with **RFC 2898 PKCS#5 Section 5.2** (FCS_CKM.1b).

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

- **RSA**, with key sizes of **2048** bits that meets the **RSA PKCS#1** standard (FCS_COP.1a); and

- **Triple-DES** with **192 bit** keys (no specific mode of operation) that meets the **FIPS-46-3** standard (FCS_COP.1b)

The mSign and EzIdentity can also generate one-time passwords (OTP) and challenge responses using the following algorithms:

- **Time OTP** (TOTP) and the **OATH Challenge Response Algorithm** (OCRA) with **160-bit** keys that meet the **RFC 4226**, **RFC 6328** and **RFC 6287** standards (FCS_COP.1d);.

The user does not directly generate these OTP, but can retrieve them via the menu option within the mSign application.

The mSign application makes use of these functions for the generation of one-time passwords that may be used by users in two-factor authentication situations. The EzIdentity 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:

- Hashing is performed via **SHA-1** and **SHA-256**, in accordance with **FIPS-180-2** (FCS_COP.1c); and

- 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 (FCS_COP.1e)

To ensure cryptographic security, the TOE is able to zeroise cryptographic keys and other sensitive data that is no longer required or in use. This is achieved by overwriting the keys and CSPs stored in memory (FCS_CKM.4).

6.5 Data Protection

The mSign application provides the functionality for the generation of RSA key pairs. These key pairs are combined with other data to produce a digital certificate. The primary function of the mSign application is to provide users with the facility to use this digital signature for the signing of transactions and other sensitive exchanges. Users are able to sign transactions to provide non-repudiation and identity assurance when performing transactions such as financial transactions and sensitive data transfer (FCO_NRO.1).

The mSign application generation One Time Passwords (OTP) to provide a two-factor EzIdentity for user authentication. These can be retrieved by users via the mSign application; the user does not contribute to the generation of these OTP.

mSign makes use of the Triple-DES algorithm to encrypt device-identifying data and mSign application data stored on a user's phone (FCS_COP.1b). 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 (FCS_COP.1c).

The TOE communicates between EzIdentity and mSign for the transmission of certificate requests, delivery data to be signed and the submission of signed data (FCO_NRO.1). This channel is logically distinct from other channels and protects the data being transmitted from modification or disclosure.

6.6 Security Management

EzIdentity provides a suite of management functions to Administrators, Super Operators and Operators. These functions allow for the configuration of both EzIdentity and mSign to suit the environment in which it is deployed. Additionally, management roles may perform the following tasks (FMT_SMF.1, FMT_MSA.1 and FMT_MSA.3):

- create users with default passwords;
- user store creation/association;
- changing of user passwords;
- import, export, enrolment of mSign credentials and tokens;
- user role management;
- user access control management;
- audit report generation; and
- Operator/Super Operator user management

Administrators may assign and adjust the functions available to Super Operators and Operators, Super Operators may assign and adjust the functions available to standard Operators (FMT_SMR.1 and FMT_MTD.1b)). These roles may access the TOE via the web portal provided by EzIdentity.

mSign users may update their PIN via the mSign application once they have authenticated with the TOE (FMT_SMR.1).

6.7 TOE Access

Both EzIdentity and mSign implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties (FDP_ACC.1, FDP_ACF.1 and FPT_ITT.1).

mSign users must authenticate with the application whenever they wish to use the digital signing, OTP or any other functionality that the application provides (FIA_UAU.2). This is achieved using a PIN set during application installation and initial configuration. Users are able to change their own PIN, the administrative roles are unable to reset a PIN if it is forgotten (FMT_MTD.1a).

mSign user sessions will be locked after a period of two minutes of inactivity (FTA_SSL.1). 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.

If a user enters an incorrect PIN 5 times, the mSign application will enter a lock state and deny any further access (FIA_AFL.1). In order to regain the functionality the application provides, the mSign user must contact an Administrator, Super Operator or Operator. They will then be able to use the EzIdentity to generate a challenge response code which will unlock the mSign application and restore functionality.

EzIdentity provides three distinct user roles – Administrator, Super Operator and Operator. Each role has differing levels of access to the functions that the TOE provides – Administrators having full access and Operators having the least (FMT_SMR.1). The functions that are available to each role are adjustable by the role above them. The interface used to access the EzIdentity is logically distinct and separate from other interfaces on the platform.

The EzIdentity will log-off a user session if the session is idle after 15 minutes. The user must then re-authenticate with the TOE prior to performing any further actions upon the TOE (FIA_UAU.2).

Depending on the configuration of the Active Directory server, EzIdentity users may become locked out from accessing the TOE after a set number of authentication attempts.