30 SEPTEMBER 2020

Document Version 1.0

MYDIGITAL ID V1.1 SECURITY TARGET

EAL3+ ALC_FLR.2

MIMOS

For more information visit us at

www.mimos.my

Document management

Document identification

Document title	MyDigital ID v1.1 Security Target
Document Version	1.0
Document date	30 SEP 2020
Release Authority	Alwyn Goh

Document history

Version	Date	Description
0.1	23-NOV-2018	Initial Released.
0.2	07-MAR-2019	Update Section 1.5 and Section 5. Change of the TOE Name to My Digital ID
0.3	18-APR-2019	Update based on new scope of TOE.
0.4	19-APR-2019	Update on the TOE name.
0.5	19-MAY-2019	Update logical scope, SFRs and descriptions.
0.6	20-NOV-2019	Update SFRs and descriptions.
0.7	16-FEB-2020	Update Section 1.6, Section 2 and Section 3.
0.8	20-SEP-2020	Update Section 1.6.2, 5.2.2, 5.2.3, 5.2.3.4.
1.0	30-SEP-2020	Final Release

Copyright notice

Table of Contents

1 Security Target Introduction

1.1 ST Reference

Table 1: Security Target (ST) Reference

ST TITLE	MyDigital ID v1.1 Security Target
ST VERSION	1.0
ST DATE	30 SEP 2020

1.2 TOE Reference

Table 2: Target of Evaluation (TOE) Reference

TOE TITLE	MyDigital ID
TOE VERSION	MyDigital ID v1.1 consist of MyDigital ID Server v1.1, and MyDigital ID Client v1.1

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 contains the security assurance requirements derived from the Common Criteria, Part 3 (ASE_REQ.2).
- Section 7 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE (ASE_TSS.1).

1.4 Defined Terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Table 3: Defined Terms

TERM	DESCRIPTION
Authentication Data	It is information used to verify the claimed identity of a user, in relation to authentication interaction or signature computation on particular transaction.
TOE Security Function (TSF) Data	Data created by and for the TOE, which might affect the operation of the TOE.
Unauthorized Users	Unauthorized users can mean a legitimate user with access rights to certain web resource, an external entity that has no rights to any protected resource or data.
User	Users of the TOE are consisting of Authorised Users.
User Data	Data created by and for the user, which does not affect the operation of the TSF.

1.5 TOE overview

1.5.1 TOE usage and major security functions

The Target of Evaluation (TOE) is MyDigital ID v1.1 and consists of MyDigital ID Client v1.1 and MyDigital ID Server v1.1. The TOE is a digital identity management and transaction signing platform. TOE provides convenient and secure method for third party mobile applications to use the digital identity of mobile.

The TOE implements the digital identity management and signing capability which is, reside as a mobile application that utilize the communication protocol and responsible for the message exchange between TOE client and TOE Server, via inter-app communication protocol on the mobile platform.

Contemporary implementations are often vulnerable, arising from various factors such as hostile applications on device, insecure communication channels and server-side storage of user credentials or keys (roaming certificates). The TOE is designed with the objective to establish trustworthiness between users and mobile service provider.

The following is the list of key features of the TOE:

- **Registration:** Users can perform registration and request for digital certificates;
- **Store Certificate:** Users can store digital certificates in the mobile devices;
- **Submit Certificate:** Users can submit certificates to the server such as authentication platform for enrolment and authentication purposes;
- **Digital Signing on File:** Users able to perform digital signing on files of any format
- **Digital Signing on hash:** Users able to perform digital signing on hash values;
- **Digital Signing on hash with proxy certificate:** Users can perform transaction signing on has values with proxy certificate. Password not required.

MyDigital ID Client

MyDigital ID client provides a secure method for third-party mobile application to use the digital Identity of mobile device users for authentication and digital signing. My Digital ID client implements the client side of MyDigital ID Protocol, and responsible for:

- Interacting with third party mobile application via inter-app communication protocol on the mobile platform.
- Processing incoming request from only authorised third-party mobile application by verifying the third-party mobile application certificate against its package name/app ID.
- Generating authorization request as specified in the MyDigital ID Protocol
- Verifying the authorisation token issued by the MyDigital ID Server as specified in the MyDIgital ID protocol.
- Generating execution token as specified in the MyDigital ID protocol.

MyDigital ID Server

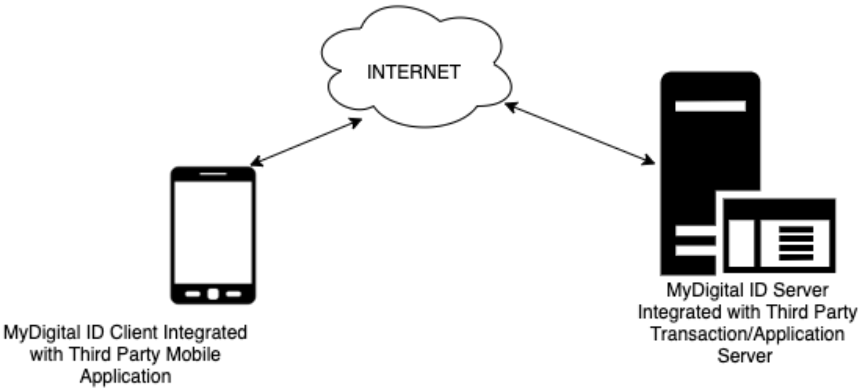
TOE Server provides capability to manage TOE users' digital certificates (through inter-communication) with third-party Transaction Server and perform cryptography processing such as key pairing and digital signature validation.

The MyDigital ID Server communicates with Third-Party Transaction Server that issues digital ID (includes of certification signing request, CSR) for the digital ID users utilize at the mobile application platforms.

MyDigital ID Server implements the server side of MyDigital ID protocol and is responsible for:

- Interacting with the third-party transaction server via socker connection to communicate MyDigital ID Protocol messages to the MyDigital ID client via a third-party mobile application.
- Processing the authorisation request generated by the MyDigital ID client.
- Generating the authorisation token as specified in the My Digital ID Protocol.
- Decrypting and verifying the execution token generated by the MyDigital ID Client
- Return transaction information to the third-party transaction server.

Deployment Scenario for MyDigital ID


INTERNET
MyDigital ID Client Integrated with Third Party Mobile Application
MyDigital ID Server Integrated with Third Party Transaction/Application Server

The following table highlights the range of security functions implemented by the TOE, as stated.

Security Feature	Description
Cryptography Operation	The TOE provides elliptic curve (EC) key-pair generation, mutual client-server authentication, digital signature generation and digital signature verification at both mobile application platforms and the digital identity Server
Identification and Authentication	The third-party mobile application interconnected with the MyDigital ID client (TOE) is required to perform successful authentication before any information flow is permitted.

Data Protection	The TOE provides a secure storage capability for user digital certificates.
Communication	The TOE is able to protect the user data from disclosure and modification using a secure protocol that defines the message exchange between MyDigital ID Client and MyDigital ID Server, via a third-party mobile application and third-party transaction server with additional security Measures. Strong security characteristics with a stringent three-pass authentication mechanism for every transaction.

Table 4: TOE Security Features

1.5.2 TOE Type

The TOE is a digital identity management and transaction signing platform. The TOE provides users access to the security features as such, digital ID secure validation and perform transaction signing using digital ID certificate at mobile platform, whilst the TOE identity server provide capability to manage TOE users digital certificates (through inter-communication) with third-party Transaction Server and perform cryptography processing such as key pairing and digital signature validation.

The TOE provides security functionality such as Cryptographic Operation, Identification and Authentication, Data Protection and Communication. The TOE can be categorised as **Products for Digital Signatures** in accordance with the categories identified on the Common Criteria Portal (www.commoncriteriaportal.org) that lists all the certified products.

1.5.3 Supporting Hardware, software and/or firmware

The underlying hardware and software that is used to support the TOE are:

Minimum System Requirements	
MyDigital ID Client	
Operating Systems	Android Platform: v4.1 iOS Platform: v9.0
MyDigital ID Server	
Operating System	Ubuntu 18.04 LTS
Processor	Dual-Core
Memory (RAM)	4GB
Disk Storage	50GB
Java Runtime Environment	1.7

Java Security Policy	128-bit key restriction shall be removed to support 256-bit key
Database	MySQL Database v5.6

Table 5: Non-TOE Firmware, Hardware and Software Specification

1.5.4 Intended method of use

The TOE is intended to be integrated with third party Service application client. The TOE components use network security protocols (i.e., SSL, TLS) to protect network data from disclosure and modification when communicating between one another, so network eavesdropping attacks on TOE communication data is significantly diminished. (The network security protocols, and all cryptographic operations used by the protocols are provided by the Operational Environment.)

1.5.5 Excluded from the TOE

The only security functionality addressed by the evaluation is the functionality specified by the functional requirements in Section 5.2, and does not include additional platform such as:

- Components specified in Section 1.5.3;
- Third-Party Mobile Application (iOS and Android); and
- Third-Party Transaction Server.

1.6 TOE description

The TOE acts as a user identity management and transaction signing (key pairing and digital signature validation) platform for the third-party mobile application to provide a secure communication. Users interact with the third-party mobile application and process request from only authorised application by verifying the third-party mobile application certificate against its package name and application identification (ID number);

1.6.1 MyDigital ID Protocol

MyDigital ID Protocol defines the message exchange between the TOE client and TOE server via a third-party transaction server. The protocol message consists of:

MyDigital ID Client

- Generate authorisation request as specified in the MyDigital ID protocol;
- Verify the authorisation token issued by the MyDigital ID server as specified in the MyDigital ID protocol; and
- Generate execution token (signed and encrypted), as specified in the MyDigital ID protocol.

MyDigital ID Server

- Interacting with the third-party transaction server via socket connection to communicate MyDigital ID protocol messages to the MyDigital ID client via third-party mobile application.
- Process the authorisation request generated by MyDital ID client.
- Generate the authorisation token as specified in the MyDigital ID Protocol.
- Verify after decryption, the execution token generated by the MyDigital client
- Return transaction information to the third-party transaction server

1.6.2 Physical scope of the TOE

The TOE consists of the following components:

- MyDigital ID Client, and
- MyDigital ID Server

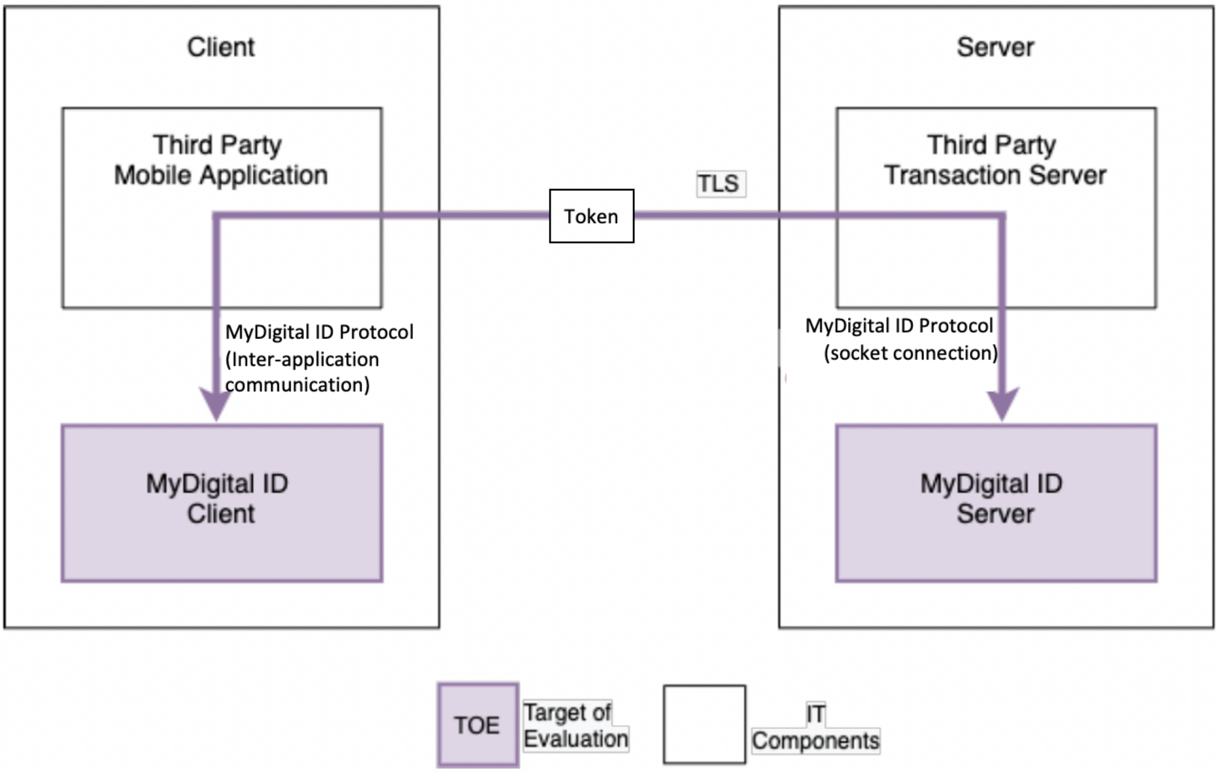

Client
Third Party Mobile Application
Token
TLS
Server
Third Party Transaction Server
MyDigital ID Protocol (Inter-application communication)
MyDigital ID Protocol (socket connection)
MyDigital ID Client
MyDigital ID Server
TOE
Target of Evaluation
IT Components

Figure 1: TOE Architecture

Referring to above figure above, illustrates the TOE operations that are consists of two main parts, which is the client, reside at mobile device platforms (iOS and Android) and a server reside at third party transaction Server or relevant server or cloud deployment.

The TOE requires third-party mobile application (service application) and third-party transaction server (service provider) to operates as a complete IT solution for client organization as digital identity management platform (known as MyDigital ID Server).

The TOE is an authentication and transaction digital ID platform that enforces authentication, authorisation, digital signing and the corresponding verification and validation processes through cryptography processes by offering mutual authentication, signature generation and correspondingly signature verification. The TOE offers signature generation, for the TOE client file and hash datatypes.

The TOE allows the specified authentication process flows to be executed via supported mobile devices (for iOS and Android), on which the TOE client is installed. The TOE client can be invoked from other mobile application (third-party service provider application) to consume the TOE security services, and furthermore leveraging its capability to provide a secure operational environment for private-key computations, inclusive of authentication and signature computation and protection of TOE Server and TOE client configuration.

Before the TOE is able to enforce any method of authentication, a user registration process is required to register all the relevant information inclusive of user identity information and the public-key linked to the TOE client. Registration of mobile users are provided by the third-party mobile application and third-party transaction server, which is out of TOE scope. Note that, all users require to complete registration process with the service provider before consume TOE services as digital ID manager.

Communication between TOE client and TOE server via MyDigital ID Communication Protocol through specific API proprietary requires by the TOE. This capability allows communication between both TOE components as well as involving communication internally between mobile applications (service provider mobile application and TOE client, as both resident on the mobile operating system) and internally at server side (between service provider transaction server and TOE server).

Note that all operations of the TOE inclusive of its installation process, management of the TOE and handling of the TOE shall be elaborated further in the Guidance documentations.

Below are the descriptions of the components stated in Figure 1 above.

Component	Description
MyDigital ID Client (TOE)	The TOE is the mobile application-server system as an authentication and transaction signing platform.
MyDigital ID Server (TOE)	The TOE Server implements the server side of MyDigital ID protocol and responsible for: i. Interacting with the third-party service provider via socket connection to communicate MyDigital ID protocol messages with the TOE application, as routed through the third-party service application and application-server connectivity; ii. Processing the authorisation request, in the form of the request token, generated by the TOE application; iii. Generating the authorisation token; iv. Processing the execution token generated by the TOE; and v. Return authentication information and status to the third-party service provider.
MyDigital ID Protocol	MyDigital ID Protocol defines the message exchange between the client and server via a third-party mobile application and third-party transaction server. It is based on three-pass authentication Mechanism MUT.CR as stated in N16813 ISO/IEC CD 9798-3.2 with additional security measures, as stated in 11700-3.11 and 11700-6.7.
Third-party Mobile Application	Third-party Mobile Application is installed on the same mobile device and interacts with the TOE application to perform authentication and signing.

Component	Description
Third-party Transaction Server	Third-party server that communicates with the TOE server, for consumption of authentication and verification services.

Table 6: TOE Components based on Figure 1

The relevant deployment and operational guidance documents for the secure operation of the TOE can be referred to MyDigital ID Technical Manual.

Section 1.5.3 lists the Operational Environment required by the TOE.

1.6.3 Logical scope of the TOE

The following is the list of TOE logical scope that defined in this document, covers by the Security Functional Requirements (SFRs).

- **Identification & Authentication.** The TOE requires that each service application is successfully Identified and authenticated before any interactions with protected resources are permitted.
- **Data Protection.** The TOE provides a secure repository capability for user's public-key certificate and configuration of the Server and Client.
- **Cryptographic Operation.** TOE also provides cryptographic functionality that utilizes the following cryptographic algorithms/functions. By using these following cryptography features, the TOE enable user to have access to authentication, signature generation and signature verification.
- **Communication.** The TOE is able to provide trusted environment and protect the user data from disclosure and modification using a communication between application and the server-side components of the TOE. The TOE is able to protect the user data from disclosure and modification using a communication protocol that defines the message exchange between MyDigital ID Client and MyDigital ID Server, via a third-party mobile application and transaction server.

2 Conformance Claim

The ST and TOE are conformant to version 3.1 (REV 5) of the Common Criteria for Information Technology Security Evaluation.

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 5 (April 2017) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 3 and Augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile

3 Security Problem Definition

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** statements that are made in terms of rules or guidelines that must be followed by the TOE and/or the operational environment.

3.2 Threats

The following is the list of threats defined by the TOE.

Table 7: Threats defined by the TOE

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. ID_SERVER	An attacker may compromise the integrity, availability and confidentially of organization information such as user information, user access credential and relevant information related to the organization by performing attacks on the authentication module.
T.MOBILE	An attacker may compromise the integrity and confidentially of sensitive data (such as access credential, cryptographic keys and etc.) stored inside the mobile devices by performing mobile application attacks.

Identifier	Threat Statement
T.DATA	An attacker (either an unauthenticated user or an unauthorised user) may impersonate an authorised user without knowing the authentication credentials to TSF data and /or user data. Plus, an attacker also can be an authorised user that tries to impersonate as another authorised user (with higher authorization or different authorisation) without knowing the authentication credentials and gain unauthorised access to TSF data and/or user data.
T.COMM	An attacker can view sensitive data (such as password) and/or manipulate data (account information) between the service application and service provider. The password that is being view by attacker can be used for attacker future authentication interactions (identity thief).

3.3 Organisational security policies

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

3.4 Assumptions

The following specific conditions are assumed to exist in an environment where the TOE is employed.

Table 8: Assumptions defined by the TOE

Identifier	Assumption Statement
A.ADMIN	The Service provider's administrator is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by MyDigital ID server documentation.
A.SERVER_OS	The operating systems supporting the TOE components protect against the unauthorised access, modification or deletion of the individual TOE components that they host.
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.NET_PORT	The environment is configured to block all traffic to the Identity access TOE server except for traffic required to perform security functionality.
A.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE.

Identifier	Assumption Statement
A.MOBILE_OS	The TOE client user shall ensure not operating on jailbroken or rooted phone.

4 Security objectives

4.1 Overview

The objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition. The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment. This section identifies the security objectives for the TOE and its supporting environment.

4.2 Security objectives for the TOE

Table 9: Security Objectives for the TOE

Identifier	Objective Statements
O.CRYPT	The TOE shall implement cryptographic functions compliant to the relevant industry standards.
O.MODIFY	The TOE shall ensure that the protected resources stored in memory are protected against unauthorised modification.
O.KEYPROTECT	The TOE shall ensure that all cryptographic keys stored within the TOE are protected sufficiently to prevent their disclosure to a malicious entity.
O.USER_ACCESS	The TOE shall ensure the only authenticated and authorised TOE Users can access the TOE functionality and protected application resources.
O.SECURE_COMM	The TOE shall ensure data exchange between client and server components satisfy confidentiality, integrity, authentication and non-repudiation requirements. It is controlled by the cryptographic support components.

4.3 Security objectives for the Environment

Table 10: 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 _SERVER	The third-party Transaction Server administrator is assigned to oversee the TOE is trusted by the organisation and are trained in use of the TOE.
OE.UPDATE	The developer shall provide updates of the TOE on a regular basis.
OE.NOEVIL	The TOE users are assumed to be non-hostile and trusted to perform all their duties in a competent manner.
OE.NET_PORT	The environment is configured to block all traffic to the TOE server except for traffic required to perform security functionality.
OE.FIREWALL	The IT environment will implement gateway filtering; only allowing HTTP and HTTPS inbound connection traffic to pass through to TOE server. The TOE server would only accept service requests from the corresponding service provider. The TOE application only accepts service requests from authorised service applications and does not have direct network connectivity.
OE.OS	The operating systems selected are of sufficient hardness to counter the perceived threats. The server-side hardness includes capabilities to establish a secure configuration to the OS, configure OS audit logs, configure proper OS authentication and permission, and ensure legacy services are not enabled.

5 Security requirements

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 (REV 5) 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 used within this ST to depict their application:

i. **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**].

ii. **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***].

iii. **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~~.

iv. **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 Identification and authentication (FIA)

5.2.1.1 FIA_AFL.1a Authentication Failure Handling (Server)

FIA_AFL.1.1a The TSF shall detect when [***1***] unsuccessful authentication attempts occur related to [**MyDigital ID client requesting MyDigital ID Server authentication**].

FIA_AFL.1.2a When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**send message to third party application to inform that the authentication has failed and terminate the request**].

Dependencies: FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

5.2.1.2 FIA_AFL.1b Authentication failure handling (Third-Party Mobile Application)

FIA_AFL.1.1c The TSF shall detect when [***1***] unsuccessful authentication attempts occur related to [**MyDigital ID Server requesting user authentication**].

FIA_AFL.1.2c When the defined number of unsuccessful authentication attempts has been [***met***], the TSF shall [**send message to third party server to inform that the authentication has failed**].

Dependencies: FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

5.2.1.3 FIA_ATD.1 User attribute definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [

- **a. Certificate corresponding to TOE-specific private-key, incorporating;**
    - **a. Corresponding public-key;**
    - **b. User identity information, inclusive of name and IC number; and**
    - **c. Certificate administrative information; and**
- b. **TOE-specific randomisation;**].

Dependencies No dependencies

Hierarchical to: No other components.

5.2.1.4 FIA_UAU.2a User authentication before any action (MyDigital ID Client)

FIA_UAU.2.1 The TSF shall require each ~~user~~ **MyDigital ID client** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

Hierarchical to: FIA_UAU.1 Timing of authentication

5.2.1.5 FIA_UAU.2b User Server authentication before any action (MyDigital ID Server)

FIA_UAU.2.1 The TSF shall require each ~~user~~ **MyDigital ID Server** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Dependencies: FIA_UID.1 Timing of identification

Hierarchical to: FIA_UAU.1 Timing of authentication

Notes: Each **system** of service application and Service provider to be successfully authenticated

5.2.1.6 FIA_UID.1a Timing of Identification (MyDigital ID Client)

FIA_UID.1.1 The TSF shall allow [***submission of authorization token by MyDigital ID Server to MyDigital ID client***] on behalf of the user to be performed before the service application is identified.

FIA_UID.1.2 The TSF shall require each ~~user~~ **MyDigital ID Client** to be successfully identified before allowing any other TSF-mediated actions on behalf of ~~that user~~ **third-party mobile application**.

Dependencies: No dependencies.

Hierarchical to: No other components.

Application Notes: Explanation of the additional authentication and identification method.

5.2.1.7 FIA_UID.1b Timing of Identification (MyDigital ID Server)

FIA_UID.1.1 The TSF shall allow [***submission of execution token by MyDIgital ID Client to MyDigital ID server***] on behalf of the user to be performed before the service application is identified.

FIA_UID.1.2 The TSF shall require ~~each user~~ **MyDigital ID Server** to be successfully identified before allowing any other TSF-mediated actions on behalf of ~~that user~~ **Third-Party Transaction Server**

Dependencies: No dependencies.

Hierarchical to: No other components.

Application Notes: Explanation of the additional authentication and identification method.

5.2.2 User Data Protection (FDP)

5.2.2.1 FDP_DAU.1 Basic Data Authentication

FDP_DAU.1.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [***document signed***].

FDP_DAU.1.2 The TSF shall provide [***signatory***] with the ability to verify evidence of the validity of the indicated information

Dependencies: No dependencies.

Hierarchical to: No other components.

5.2.2.2 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the [**access control SFP**] on [**Subject: authorise user, Object: password, operation: perform signing, generate encryption key and encrypt execution token at My Digital ID Client**]

Dependencies: FDP_ACF.1 Security attribute-based access control

Hierarchical to: No other components.

5.2.3 Cryptographic Support (FCS)

5.2.3.1 FCS_COP.1a Cryptographic operation (digital sign)

FCS_COP.1.1 The TSF shall perform [**digital signature creation and verification**] in accordance with a specified cryptographic algorithm [

a) **ECDSA with SHA-2,**

] and cryptographic key sizes [

a) **ECDSA using secp256r1 curve of 256 bits over F_p and SHA-2 256 bits,**

] that meet the following: [

a) **PKCS #7]**

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

Hierarchical to: No other components.

Notes: The primary purpose of the TOE is to enable the establishment and management of a public key infrastructure. Digital signature cryptography is a critical component of the PKI systems that are established by the TOE providing the basis for trust in the management of digital certificates.

5.2.3.2 FCS_COP.1b Cryptographic operation (symmetric)

FCS_COP.1.1 The TSF shall perform [**symmetric encryption and decryption**] in accordance with a specified cryptographic algorithm [

a) **AES,**

] and cryptographic key sizes [

a) **256 bit (AES),**

] that meet the following: [

a) **FIPS-197**

].

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

Hierarchical to: No other components.

5.2.3.3 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [

a) **AES,**

b) **ECDSA**

c) **ECDH**

] and specified cryptographic key sizes [

a) **256 bit (AES),**

b) **256 (ECDSA)**

c) **256 (ECDH)**

] that meet the following: [

a) **FIPS-197**

b) **ANSI X9.62-2005**

c) **ISO/IEC 11770-3:2015]**

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

Hierarchical to: No other components.

5.2.3.4 FCS_CKM.2 Cryptographic key distribution

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [

a. X.509 public key certificate in PKCS#7 format,

b. PKCS#10 certificate request

] that meets the following: [

a. [PKCS7],

b. ***[PKCS10]***].

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

Hierarchical to: No other components.

5.2.3.5 FCS_CKM.4 Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**memory overwrite**] that meets the following: [**none**].

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]

Hierarchical to: No other components.

5.2.4 Secure Communication (FCO)

5.2.4.1 FCO_NRO.1a Selective proof of origin (MyDigital ID Client)

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

Hierarchical to: No other components.

5.2.4.2 FCO_NRO.1b Selective proof of origin (MyDigital ID Server)

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

Hierarchical to: No other components.

5.3 Rationale

The following is the list of rationale for the declaration and selection of Security Functional Requirement (SFR) towards the Security Problem Definition (SPD), through defined rationale justifications.

5.3.1 Security Objectives of the TOE Rationale

The following is the mapping between Security Objectives of the TOE towards the Security Problem Definition define in this document.

Table 11: SFR Rationale for Security Objectives

Objectives	SFR	Rationale
O.CRYPT	FCS_COP.1a FCS_COP.1b	O.CRYPT meets the requirement by providing algorithms for cryptographic operation, which can be used to encrypt, decrypt, digital signature, digital signature verification on the data passing through or being stored on the TOE, or data passing between the TOE and an external device.
	FCS_CKM.4	The requirement helps meet the objective by destroying cryptographic keys in accordance with a specified cryptographic key destruction method.
O.MODIFY	FDP_DAU.1 FDP_ACC.1	O.MODIFY meets the requirement by ensuring basis of authentication are applied for any activities performed by the TOE specifically for digital signing on the document selected.
O.KEYPROTECT	FCS_CKM.1 FCO_NRO.1a	O.KEYPROTECT meets the requirement by generating a cryptographic to secure the data for the transfer.
	FCS_CKM.2 FCO_NRO.1b	O. KEYPROTECT meets the requirement by ensuring the method of key distribution and storage are secure based on the configuration algorithm, algorithm requirements and processing are applied.
	FDP_ACF.1 FDP_ACC.1	O.KEYPROTECT meets the objective by enforcing the [access control SFP] to objects which defined by the TSF .
O.USER_ACCESS	FIA_UID.1a FIA_UID.1b	O.USER_ACCESS meets the requirement by allowing authentication methods on behalf of the user to be performed before the user is identified.
	FIA_AFL.1a FIA_AFL.1b	O.USER_ACCESSS Is fulfilled by detect invalid login attempt to the TOE. And is fulfilled by limit access of unauthorized user to access the TOE. The account will be disabled if invalid credentials have met the maximum attempts allowed.

Objectives	SFR	Rationale
	FIA_ATD.1	The requirement meets the objective O.USER_ACCESSS by defining the attributes from TOE Users authentication.
	FIA_UAU.2a FIA_UAU.2b FIA_UID.1a FIA_UID.1b	The requirement meets the objective O.USER_ACCESS by allowing authentication methods on behalf of the user to be performed before the user is identified.
O.SECURE_COMM	FCO_NRO.1a FCO_NRO.1b	The requirement meets the objective O.COMM by exporting data with security attributes which provide capability to verify the evidence of origin, which is in addition required by selective proof of origin.

Table 12: Threats Rationale for Security Objectives for the TOE

Objectives	Threat	Rationale
O.CRYPT	T.DATA	The TOE security functions based on the SFR justification able to ensure that the TOE protects the TSF data and User data from any modification through cryptographic processes.
O.MODIFY	T.MODIFY	The TOE security functions based on the SFR justification able to ensure that the TOE protects the TSF data and User data from any modification through relevant access control.
O.KEYPROTECT	T.DATA T.COMINT T.COMM	The TOE security functions based on the SFR justification able to ensure that the TOE protects the cryptographic keys from any modification through key validation, key verification and secure communication.
O.USER_ACCESS	T.COMM T.MOBILE T.ID_SERVER	The TOE security functions based on the SFR justification able to ensure that the TOE protects the TSF data and User data via user access credentials on mobile app or web app from any modification, bypassing or compromise integrity.

Objectives	Threat	Rationale
O.SECURE_COMM	T.COMM	The TOE security functions based on the SFR justification able to ensure that the integrity and confidentiality of exchanged data between the TOE client and TOE Server.

5.3.2 Security Objectives of the TOE Operational Environment Rationale

The following is the mapping between Security Objectives of the TOE towards the Security Problem Definition define in this document.

Table 13: Assumption Rationale for Security Objectives for the TOE Operational Environment

Objectives	Assumption	Rationale
OE.INSTALL	A.SERVER_OS A.UPDATE	OE. INSTALL fulfilled the assumptions by ensuring the TOE underlying operating system and application are delivered, installed, configured and patched up based on documented to ensure security on the TOE implementations.
OE.ADMIN_SERVER	A.ADMIN	OE. ADMIN fulfilled the assumption by ensuring the TSF are selected among the competent staff, negligent, non-hostile and passed all security vetting based on organization policies requirements.
OE.OS	A.SERVER_OS A.UPDATE A.MOBILE_OS	OE.OS fulfilled the assumptions by ensuring the TOE underlying operating system and application are delivered, installed, configured plus patched up based on documented to ensure security on the TOE implementations. The third-party mobile application shall ensure not operating on jailbroken or rooted phone.
OE.UPDATE	A.SERVER_OS A.UPDATE	OE. OS fulfilled the assumptions by ensuring the TOE underlying operating system and application are delivered, installed, configured plus patched up based on documented to ensure security on the TOE implementations.
OE.NOEVIL	A.ADMIN	OE. ADMIN fulfilled the assumption by ensuring the TSF are selected among the competent staff, negligent, non-hostile and passed all security

Objectives	Assumption	Rationale
		vetting based on organization policies requirements.
OE.NET_PORT	A.NET_PORT	OE.NET_PORT fulfilled the assumption by blocking any unauthorized traffic except for that traffic allowed as per configured by service provider administrator according to organization policies.
OE.FIREWALL	A.FIREWALL	OE. FIREWALL fulfilled the assumption by providing network filtering at the gateway through configuration of HTTPS and HTTP defined by the organization.

5.4 TOE Security Assurance Requirements

EAL3+ ALC_FLR.2 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.

EAL3+ ALC_FLR.2 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 on the architecture of the TOE, to understand the security behaviours.

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 attackers with basic attack potential.

EAL3+ ALC_FLR.2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Table 14: SAR

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.3 Functional specification with complete summary
	ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.3 Authorisation controls
	ALC_CMS.3 Implementation representation CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_FLR.2 Flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction

Assurance Class	Assurance Components
	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
	ATE_FUN.1 Functional testing
	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.4.1 Assurance Requirements Rationale

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 3 (EAL3). The 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.

This EAL was chosen based on the security problem definition and the security objectives for the TOE. The TOE is intended to address the common authentication and authorization attacks on the

Thus, provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour.

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

5.5 TOE Summary Specification

5.5.1 Overview

This section provides the TOE summary specification in which, illustrates the mapping of justifications on the TOE security functions in achieving the consistency with the logical scope of the TOE. Thus, the following mapping that leads with the scope of TOE shall justify the requirements of SFRs defined.

5.5.2 Mapping of TOE Logical Scope towards the SFRs

The following the descriptions of mapping between TOE logical scope with the list of Security Functional Requirements (SFRs) defined in this document. Whilst, this mapping shall elaborate the components of the TOE defined in the Logical Scope are meeting the SFRs as per required by the CEM.

Table 15: Mapping between Logical Scope and SFRs

Logical Scope	Security Functional Requirement (SFR)
Identification and Authentication	FIA_AFL.1a FIA_AFL.1b FIA_ATD.1 FIA_UAU.2a FIA_UAU.2b FIA_UID.1a FIA_UID.1b
Data Protection	FDP_DAU.1 FDP_ACC.1
Cryptographic Operation	FCS_COP.1a FCS_COP.1b FCS_CKM.1 FCS_CKM.2 FCS_CKM.4
Communication	FCP_NRO.1a FCP_NRO.1b

5.5.2.1 My Digital ID Operation

5.5.2.2 Identification and Authentication

The TOE shall enforce security login through the identification and authentication processes where TOE user shall provide valid username and password as login credential. The TOE protects all relevant data and configuration related to TOE operations as well users in the TOE registration database, whilst enforcing secure authentication through username and password, plus additional factor of authentication may applied based on the organization policy and procedures.

The TOE interacts with third-party mobile applications via inter-app communication protocol to process the incoming request from the applications such as initiation request, authorisation request and token authorisation. The TOE requires each third-party mobile applications to be successfully identified and authenticated before allowing any other TSF-mediated actions. The TOE implement access control and authentication measures to ensure that TOE data and functionality is not misused by unauthorised parties. The TOE processed incoming request from authorised third-party mobile applications by verifying certificate against its package name or application ID

All third-party mobile applications must provide authentication data to the TOE to affirm their identity and role prior to being granted access to any TOE functions or interfaces.

Mobile users are being registered first in the TOE Server and assigned with username, password and other factor authentication (if applicable) accordingly..

Each login attempts supported with MyDigital ID protocol in between TOE client user and TOE Server. Details of the TOE operations of the identification and authentication functions of the TOE, kindly refer to TOE Guidance documentations.

5.5.2.3 Data Protection

Upon TOE User registration, each of that information are manage accordingly by TOE server in its secure operational environment. Furthermore, the access to those information and configuration only being given to authorized Service Provider administrator.

The TOE provide a capability to generate evidence that can be used as a guarantee of the validity of signed document and provide [signatory] with the ability to verify evidence of the validity of the indicated information.

The TOE also able to generate evidence of origin for the transmitted digital certificates at the request of the recipient and to the recipient. The TOE has the ability 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. 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.

Furthermore, in the management of the TOE, configuration of the TOE Server and TOE client holds by the TOE Server under the purview of TOE Server, through the advice and guidance of organization security policies. In ensuring all the configuration of the TOE Server maintained accordingly based on define organization security policies and procedures, the TOE protects those configurations through limited accessibility to only TOE Server.

In the aspects of operations in the TOE client, all relevant updates, upgrades, patches, security policies configurations and security protection configuration are being send to assigned registered TOE client through the advisory informed by TOE Server. This is to ensure there are in tampering prevention on those configurations either at TOE Server and TOE client thus allowing security policies and procedures applied both sides.

Details operations of the user data protection functions of the TOE, kindly refer to TOE Guidance documentations.

5.5.2.4 Cryptographic Operation

TOE provides a cryptographic library to generate and perform ECDSA with SHA-2, AES, ECDSA, ECDH. The TOE also distributes cryptographic public keys such as X.509 public key certificate in PKCS#7 format and PKCS#10 certificate request.

The TOE provides a secure key archival and retrieval capability for end users' private encryption keys; this enables an end user to recover a key at a later date should the user's copy of the key become corrupt or lost. It also enables an organization to recover encrypted data if a key/certificate owner leaves the company unexpectedly. The TOE provides key archival and key recovery functions through the encryption of the private encryption key with a random symmetric key.

The TOE also performs key destruction by overwriting the memory space of the keys. This function overwrites the previous keys when the user deletes the expired certificate(s) and key(s).

5.5.2.5 Communication

TOE provide communication Protocol from TOE Digitial ID Server towards those TOE clients and vice versa, this is to ensure the TOE as whole solution are not being compromise or data being tampered in its operations along the way. Transmission of data from TOE Server especially the PUSH commands via proprietary API protocols of MyDigital ID shall be securely applied and preventing from being bypass, sniffed and tampered.

With that, between the TOE Server and TOE Client, but not limited to TOE Users, the communication shall be protected via proprietary API protocols of MyDigital ID to ensure not being bypassed or sniffed. Preventing attacker to access the TOE and made unauthorized changes.

Details operations of the communication functions of the TOE, kindly refer to TOE Guidance documentations.

END OF DOCUMENT