06 NOV 2020
Document Version 1.0

DSONIC EID SECURITY TARGET

DATASONIC

For more information visit us at

www.datasonic.com.my

Document management

Document identification

Document title	Dsonic eID Security Target
Document date	06-NOV-2020
Document version	1.0
Release Authority	Datasonic Smart Solutions Sdn. Bhd.

Document history

Version	Date	Description
0.1	20-AUG-2019	Initial Released by Securelytics GRCC
0.2	05-JUNE-2020	Added TOE Summary Specification in Section 6
0.3	20-JULY-2020	Updated Section 1, Section 5 and Section 6
0.4	24-JULY-2020	Updated Section 1, Section 5, 6 based on developer's comment
0.5	07-AUG-2020	Updated Section 1.5 and Section 6.2
1.0	06-NOV-2020	Updated Section 1 until Section 6 based on evaluator's and certifier's comments Final Released

Copyright notice

Table of Contents

1 Security Target Introduction

1.1 ST Reference

Table 1: Security Target (ST) Reference

ST TITLE	Dsonic eID Security Target
ST VERSION	1.0
ST DATE	06-NOV-2020

1.2 TOE Reference

Table 2: Target of Evaluation (TOE) Reference

TOE TITLE	Dsonic eID Platform which consist of: • Dsonic eID Server • Dsonic eID Key Management Service (KMS)
TOE VERSION	Dsonic eID Platform which consist of: • Dsonic eID Server v1.1.0 • Dsonic eID Key Management Service (KMS) v1.0.0

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 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

TERMS	DESCRIPTIONS
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.
CA	Certificate Authority
CM	Configuration Manager
CSR	Certificate Signing Request
ECC	Elliptic-curve cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
eKYC	Electric Know-Your-Customer
HSM	Hardware Security Module
RSA	Rivest-Shamir-Adleman cryptography algorithm
SHA	Secure Hash Algorithms
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 Dsonic eID Platform which consist of Dsonic eID Server v1.1.0 and Dsonic eID Key Management Service (KMS) v1.0.0. The TOE is an integrated platform for trusted digital identity and serve as a digital identity management and authorising platform. It involves registration and generation of a single trusted digital ID that can be used for e-government and e-commerce services. It is a next generation platform that able to digitise and strengthen existing security document such as digital MyKad (Identity Card) and digital driving license.

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

- PKI-Based Authentication – The TOE provides a security infrastructure that issues and manages token and digital certificates. Digital certificate can be used to sign document digitally.
- eKYC Identification - A streamlined eKYC experience by offering a simple and digitalized version of normal KYC procedure where verification strategy is performed electronically via Facial Recognition.
- Single Sign-On Across Platform – Single Sign-On allows users to access multiple services without repeating the registration process. User does not need to repeatedly enter basic identity information such as Name, IC number, Address, Date of birth and others to register for various digital services. The TOE enabled identity validation and user authentication with greater convenience.
- Document Signing – Document Signing support online transactions approval with digital signing without in-person presence. It is an authentication-based signature-related processes by applying electronic signatures on the documents hash value. It can later be verified by the receiver that the document has not been modified after signing.

The following table highlights the range of security functions implemented by the TOE:

Table 4: TOE Security Features

SECURITY FEATURES	DESCRIPTIONS
Digital ID and Cryptographic Operations	The TOE provides cryptographic functionality that utilizes several cryptographic algorithms in order to generate cryptography key pair, generate digital certificates and perform digital ID operations such as PKI-based authentication, digital signature generation and verification, single sign-on and digital document signing (signing on the document hash value).
Identification and Authentication	Third party services integrated with the Digital ID application provider will also be identify and authenticate before they could allow user to perform Single Sign-on and obtained user information.
Data Protection	The TOE provides a secure retrieval capability for user digital certificates.

SECURITY FEATURES	DESCRIPTIONS
Secure Communication	The TOE provides a secure communication of user data from disclosure and modification between the third-party mobile application and the server-side components of the TOE and also between Dsonic eID server and Dsonic eID KMS

1.5.2 TOE Type

The TOE is an integrated platform for trusted digital identity and serve as a digital identity management and authorising platform. The TOE provides several security features as such Digital ID and Cryptographic Operations, Identification and Authentication, Data Protection and Secure 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:

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

Minimum System Requirements	
Dsonic eID Server	
Operating Systems	Windows Server 2018 or latest
Processor	Intel Xeon / AMD EPYC
Memory (RAM)	4GB or above
HDD Storage (MB)	50GB or above
Core	4 or Above
Network	Gigabit (10/100/1000baseT) Ethernet adapter
Internet	Broadband access (1Gbps or above)
Software	
Internet Information Services (IIS)	10.0 or latest
.NET Core	3.1
Database	MySQL v5.7.22 or latest
Dsonic KMS Server	
Operating Systems	Linux
Processor	Intel Xeon / AMD EPYC
Memory (RAM)	4GB
HDD Storage (MB)	30GB or Above
Core	4 or Above
Network	Gigabit (10/100/1000baseT) Ethernet adapter
Software	

NodeJS	LTS version 10.0 or latest
EJBCA	6.10.1
Enterprise customer or agency client application / Third-Party application	
Mobile Platform	Android Platform: 4.1 or latest
Web Browser	Microsoft Edge 44 and later Mozilla Firefox 64 and later Google Chrome 71 and later Safari 14 and later

1.5.4 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:

- Third-Party Application (Mobile/Web Application)
- Enterprise Customer/ Government Agency Application (Mobile/Web Application)

1.6 TOE Description

1.6.1 Physical Scope of the TOE

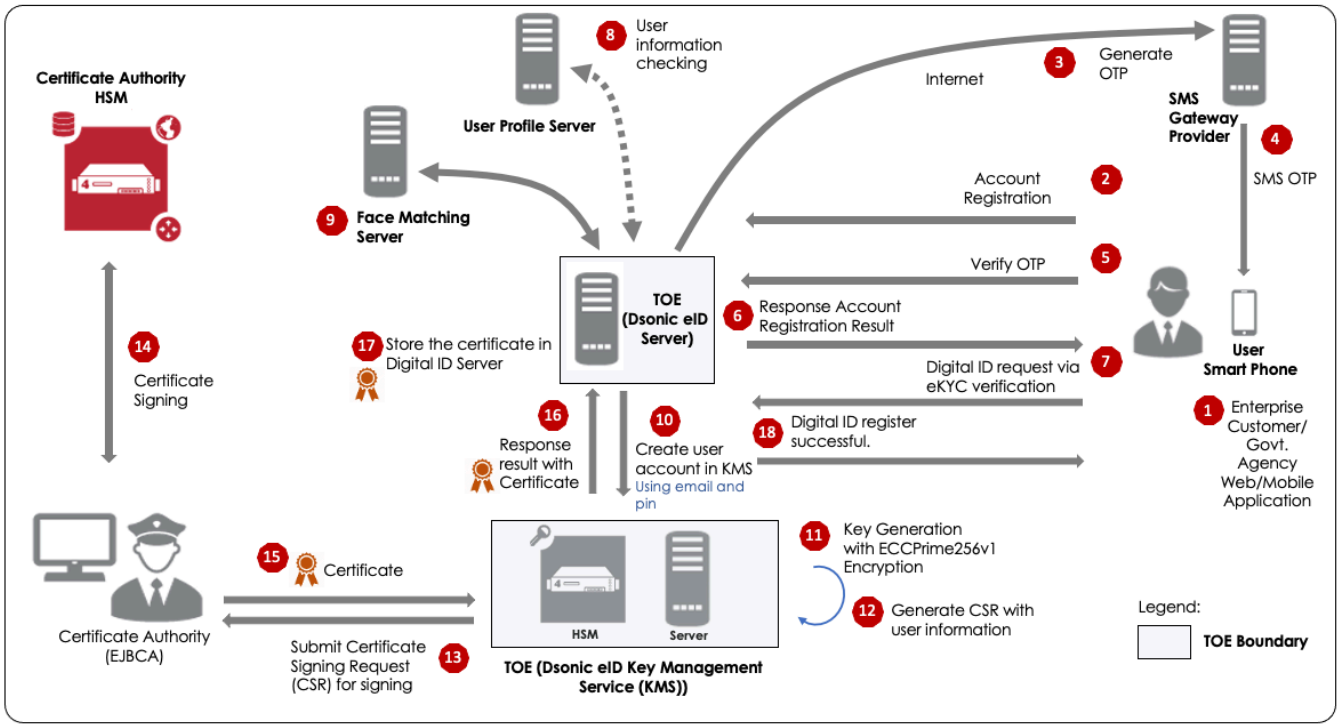

Figure 1: TOE Architecture

The TOE is a complete platform for enterprises or government agency to manage and perform verification/authentication of digital identities in a reliable, secure and convenient manner. Figure 1 above illustrates the TOE operations. Enterprise customer or government agency who build their own digital identity mobile application can use the TOE via API integration.

Below is the Digital ID registration process flow:

1. User need to perform Digital ID registration using enterprise customer or agency mobile application by providing several information (e.g. IC number, Phone number and login password)
2. The registration request will be sent to the Dsonic eID Server (TOE) via API.
3. The Dsonic eID Server (TOE) will send a request to SMS gateway provider to send an OTP number to the user's mobile phone
4. SMS Gateway send OTP to user's mobile phone
5. User send the OTP via the third-party mobile application to Dsonic eID Server (TOE) for verification
6. User account will be created in the Dsonic eID Server (TOE) once OTP has been verified successfully
7. User request to create Digital ID by performing eKYC verification at the enterprise customer or agency mobile application. eKYC is a procedure to identify and verify a customer's identity by uploading their selfie and IC card picture for verification.

8. User information (e.g. IC number, name and address) will be verified against the data in enterprise customer or agency User Profile Server, additional data such as image will be grab from the enterprise customer User Profile Server.
9. Image data from the enterprise customer or agency User Profile Server will be uploaded to the Face Matching Server to perform facial matching against User Selfie data.
10. Once all data verified successfully, a key user account will be created in Dsonic eID KMS (TOE) using the user's email and pin data.
11. Dsonic eID KMS (TOE) will perform key generation using ECC algorithm
12. The key then will be used to generate CSR with the user information
13. Then the CSR will be submitted to CA for signing.
14. CA will use their HSM to perform the certification signing
15. User certification will be returned to the Dsonic eID KMS (TOE)
16. Dsonic eID KMS (TOE) will submit the digital certificate to Dsonic eID Server (TOE)
17. Dsonic eID Server (TOE) will store the certificate
18. Digital ID registration successful

Note that all operations of the TOE inclusive of its preparational and API integration process will be elaborated further in the Guidance documentation.

The TOE delivery will be practising **On Premise** distribution strategy, whereby the TOE will be delivered together with servers with the TOE pre-installed. This model ensures reliable performance and data security for highly sensitive data.

1.6.2 Logical Scope of the TOE

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

- **Digital ID and Cryptographic Operations:** TOE provides cryptographic functionality that utilizes ECC algorithm and RSA algorithm. By using these cryptography features, the TOE enables users to perform PKI-based authentication, digital signature generation and verification, single-sign on and digital document signing (signing on the document hash value).
- **Identification & Authentication.** Third party services integrated with the Digital ID application provider will also be identify and authenticate before they could allow user to perform Single Sign-on and obtained user information.
- **Data Protection.** The TOE provides a secure retrieval capability for user digital certificates.
- **Secure Communication:** The TOE is able to protect the user data from disclosure and modification using a secure communication between application and the server-side components of the TOE.

2 Conformance Claim

The ST and TOE are conformant to version 3.1, Revision 5, April 2017 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, Revision 5, April 2017

- **Part 3 conformant**. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 5, April 2017. The claimed assurance package is EAL2 augmented with ALC_FLR.2.

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 6: Threats defined by the TOE

IDENTIFIERS	THREAT STATEMENTS
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.
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.

IDENTIFIERS	THREAT STATEMENTS
T.COM	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 7: Assumptions defined by the TOE

IDENTIFIERS	ASSUMPTION STATEMENTS
A.ADMIN	The Administrator is not careless, wilfully negligent, or hostile, and will follow and abide by the instructions provided by administrator documentation.
A.OPSYS	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 management server (TOE) 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.
A.OS	The TOE administrator shall ensure the OS Backend Server have been hardened to counter the perceived threats.

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 8: Security Objectives for the TOE

IDENTIFIERS	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.
O.CRYPT	The TOE shall implement cryptographic functions compliant to the relevant industry standards.

4.3 Security Objectives for the Environment

Table 9: 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 TOE 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.
OE.UPDATE	The developer shall provide updates of the TOE on a regular basis.
OE.NOEVIL	The TOE administrator and 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:

- **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
FIA_ATD.1	User attribute definition
FIA_UID.2	Third-party application identification before any action
FIA_UAU.2	Third-party application authentication before any action
FDP_DAU.1	Basic Data Authentication
FCS_CKM.1	Cryptographic key generation
FCS_CKM.2	Cryptographic key distribution
FCS_CKM.4	Cryptographic key destruction
FCS_COP.1	Cryptographic Operation
FCO_NRO.1	Selective proof of origin
FTP_TRP.1	Trusted Path

5.2.2 FIA_ATD.1 User attribute definition

FIA_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to ~~users~~ enterprise customer or agency **application**: [• **Enterprise customer or agency application users' private-key and public-key;** • **Enterprise customer or agency application users' digital certificate;** • **Certificate administrative information, inclusive of issuance date, expiry date and revocation information;** • **Third-party application users' identity information, inclusive of Name, IC number, Mobile Number, Password;** • **Device ID**].
Dependencies	No dependencies
Hierarchical to	No other components.

IDENTIFIER	TITLE
Notes	None

5.2.3 FIA_UAU.2 ~~User~~ Third-party application authentication before any action

FIA_UAU.2.1	The TSF shall require each ~~user~~ **third-party application** to be successfully authenticated before **enterprise customer or agency application** 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	None

5.2.4 FIA_UID.2 ~~User~~ Third-party application authentication before any action

FIA_UAU.2.1	The TSF shall require each ~~user~~ **third-party application** to be successfully identified before **enterprise customer or agency application** allowing any other TSF-mediated actions on behalf of that user.
Dependencies	No dependencies
Hierarchical to	None
Notes	None

5.2.5 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.
Notes	None

5.2.6 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) RSA,** **b) ECC P-256 and P-384**] and specified cryptographic key sizes [**a) 1024, 2048 or 3072 bit (RSA),** **b) between 160 and 571 bits over F_p and F_{2m} (ECC)**] that meet the following: [**c) PKCS #1 (RSA)** **d) ANSI X9.62-2005 (ECC)]**
Dependencies	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction
Hierarchical to	No other components.
Notes	None

5.2.7 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. [PKCS #7],** **b. [PKCS #10]**].
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	None

5.2.8 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.
Notes	None

5.2.9 FCS_COP.1 Cryptographic operation

FCS_COP.1.1	The TSF shall perform [**digital signature creation and verification**] in accordance with a specified cryptographic algorithm [**a) RSA** **b) ECC P-256 and P-384,**] and cryptographic key sizes [**a) RSA 1024, 2048 or 3072** **b) ECC using curves between 160 and 571 bits over F_p and F_{2m}**] that meet the following: [**a) PKCS #1** **b) ANSI X9.62-2005**
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:	None

5.2.10 FCO_NRO.1 Selective proof of origin

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.

5.2.11 FTP_TRP.1 Trusted Path

Hierarchical to:	No other components.
FTP_TRP.1.1	The TSF shall provide a communication path between itself and [***remote***] ~~users~~ **IT Systems** that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [***modification or disclosure***].
FTP_TRP.1.2	The TSF shall permit [***remote IT Systems***] to initiate communication via the trusted path
FTP_TRP.1.3	The TSF shall require the use of the trusted path for [***initial third-party application authentication***, [**and all further communication after authentication**]].
Dependencies	No dependencies
Notes	None.

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 10: SFR Rationale for Security Objectives

Objectives	SFR	Rationale
O.CRYPT	FCS_COP.1	This requirement supports O.CRYPT 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.
O.MODIFY	FDP_DAU.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.1	O.KEYPROTECT is fulfilled by generating a cryptographic to secure the data for the transfer.
	FCS_CKM.2 FCO_NRO.1	O.KEYPROTECT is fulfilled by ensuring the method of key distribution and storage are secure based on the configuration algorithm, algorithm requirements and processing are applied.
	FTP_TRP.1	O.KEYPROTECT is fulfilled by which ensures that traffic transmitted between TOE components is protected from disclosure and modification
O.USER_ACCESS	FIA_ATD.1	The requirement meets the objective O.USER_ACCESSS by defining the attributes from TOE Users authentication.
	FIA_UAU.2 FIA_UID.1	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.

Table 11: 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.

Objectives	Threat	Rationale
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.COM	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.COM T.MOBILE T.WEB_SVR	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.

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 12: Assumption Rationale for Security Objectives for the TOE Operational Environment

Objectives	Assumption	Rationale
OE.INSTALL	A.OS A.UPDATE	OE.INSTALL 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.ADMIN	A.ADMIN	OE.ADMIN fulfilled the assumption by ensuring the TOE administrator are selected among the competent staff, negligent, non-hostile and passed all security vetting based on organization policies requirements.
OE.OS OE.OPSYS	A.OS A.OPSYS A.UPDATE	OE.OS and OE.OPSYS 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.

Objectives	Assumption	Rationale
OE.UPDATE	A.OS A.UPDATE	OE.UPDATE fulfilled the assumptions by ensuring the TOE underlying operating system and application are updated on a regular basis.
OE.NOEVIL	A.ADMIN	OE.ADMIN fulfilled the assumption by ensuring the TOE administrator are selected among the competent staff, negligent, non-hostile and passed all security 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 TOE 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

EAL2 augmented with 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.

EAL2 augmented with 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.

EAL2 augmented with ALC_FLR.2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

Table 13: SAR

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
	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
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition

Assurance class	Assurance components
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
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 2 (EAL2) augmented with ALC_FLR.2. 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 web-based applications.

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 a Basic attack potential.

6 TOE Summary Specification

6.1 Overview

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

- Digital ID and Cryptographic Operation;
- Identification and Authentication;
- Data Protection;
- Secure Communication

6.2 Digital ID and Cryptographic Operations

The TOE performs key generation using RSA cryptographic algorithm with 1024, 2048 or 3072 cryptographic key sizes and ECC P-256/P-384 using curves between 160 and 571 bits over Fp and F2m (FCS_CKM.1). For key distribution, the TOE shall be able to distribute the keys in X.509 public key certificate in PKCS#7 format and PKCS#10 certificate request key distribution method (FCS_CKM.2). The TOE also able to destroy cryptographic keys by performing memory overwrite (FCS_CKM.4). The TOE performs a digital signature creation and verification using RSA cryptographic algorithm with 1024, 2048 or 3072 cryptographic key sizes and ECC P-256/P-384 using curves between 160 and 571 bits over Fp and F2m (FCS_COP.1).

By using these cryptography features, the TOE enables users to perform PKI-based authentication, digital signature generation and verification, single-sign on and digital document signing (signing on document hash value). The TOE also uses these cryptographic algorithms to generate cryptography key pair and secure the transaction communication.

6.3 Identification and Authentication

The 3rd party mobile/web application integrated with the TOE enterprise customer or agency application is required to perform successful identification and authentication before any information flow is permitted (FIA_UAU.2, FIA_UAU.2).

The TOE maintains enterprise customer or agency application users' private-key and public-key, enterprise customer or agency application users' digital certificate, Certificate administrative information, inclusive of issuance date, expiry date and revocation information, enterprise customer or agency application users' identity information, inclusive of Name, IC number, Mobile Number, Password and Device ID (FIA_ATD.1).

6.4 Data Protection

Evidence (certificates) will be generated to guarantee the validity of document signed. The signatory has the ability to verify evidence of the validity of the indicated information (FDP_DAU.1). The TOE also able to generate evidence (certificates) of origin for transmitted at the request of the recipient and verify the evidence of origin of information to recipient given that the information is digitally signed or protected. The TOE is capable 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).

6.5 Secure Communication

The TOE provides a secure communication of user data from disclosure and modification using a secure communication between application and the server-side components of the TOE. The TOE provides a secure communication of user data from disclosure and modification between the third-party mobile application and the server-side components of the TOE and also between Dsonic eID server and Dsonic eID KMS. The TOE implements the TLS v1.2 protocol (FTP_TRP.1)