insight to !nspiration

SDS FIDO V1.1 Security Target Lite

Sep 2, 2015

Solution Group (SC_MA)
Smart Convergence
Business Unit

SAMSUNG SDS SAMSUNG

Contents

List of Figures

List of Tables

1 Security Target Instruction

This document is the security target of SAMSUNG SDS FIDO(Fast Identity Online) Server Solution V1.1, which is developed by Samsung SDS Co., Ltd.(Hereafter: SDS).

1.1 Security Target Reference

- Subject: SAMSUNG SDS FIDO Server Solution V1.1 Security Target
- Document version: V2.0
- Date: 2 Sep 2015
- Author: Samsung SDS
- Evaluation Criteria: Common Criteria for Information Technology Security Evaluation V3.1r4
- Evaluation Assurance Level: EAL2 (International)
- Protection Profile: none

1.2 TOE Reference

- Developer: SAMSUNG SDS Solution Group (SC_MA)
- TOE: SAMSUNG SDS FIDO Server Solution V1.1
- Component of TOE:
  - SDS FIDO Server V1.1.1(12)(Hereafter: FIDO Server)
  - SDS FIDO Admin Portal V1.1.1(12)(Hereafter: Admin Portal)
  - FIDO_Application Developer Manual(Server)_V1.1_KOR
  - FIDO_Application Developer Manual(Client)_V1.1_KOR
  - FIDO_Manager Manual_V1.1_KOR
  - FIDO_Install Manual_V1.1_KOR
  - FIDO_User Manual_V1.1_KOR

1.3 TOE Overview

1.3.1 Usage and Major Security Features of the TOE

TOE, SAMSUNG SDS FIDO Server Solution V1.1, is a authentication system that authenticates a user by connecting to a FIDO Server (Hereafter; TOEs), which is an online environment, if the user's own biometrics information recognition from device is successful. Biometrics information is never transmitted to or stored in TOEs. Available TOE operation environment devices are Samsung Galaxy S6 and Samsung Galaxy S6 edge using fingerprint. FIDO Client, Authenticator[1], and ASM (Authenticator-Specific Module) Application are pre-loaded in Galaxy S6 and Galaxy S6 edge.

TOE can be used as identification authentication and non-repudiation method for service users of Service Provider (Hereafter; SP). SP provides SP Server that interfaces with TOEs and SP App, which is installed in a device. Service that can implement TOE includes mobile banking, app card, securities mobile trading system, insurance mobile sales support system, mobile shops, government and public office application service, enterprise mobile intranet and etc. Service users use the user authentication through TOEs connected to SP Server using the SP App that have been used.

The communication between TOEs and FIDO Client follows UAF Protocol Specification (Universal Authentication Framework specs published on 2014-12-09) from FIDO Alliance [2]based on public key infrastructure (PKI).

Differently from general public key infrastructure, Attestation Private Key and Attestation certificate are pre-stored in the Secure Storage where only Authenticator can access.

A large number of authenticators sharing the same Attestation Certificate provide better privacy. However, user's public key and private key that are generated by the Authenticator during registration for the local device, online service (SP) and user's account. User's public key is sent to TOEs and associated with the user's account. The private key and any information about the local authentication method (such as biometric measurements or templates) never leave the local device [7]. SP App and SP Server communicate through TLS1.2 via UAF Protocol Message. UAF Operations defined by UAF Protocol Specification, such as Registration, Authentication, Transaction Confirmation, Deregistration can be operated in TOE operation environment.

When service user requests registration, Authenticator digitally signs the registration data object with Attestation Private Key. TOEs verifies the transmitted digital signature with Attestation Public Key. When service user requests authentication, Authenticator digitally signs the authentication data object with user's private key stored in the secure storage. TOEs verifies the transmitted digital signature with user's Public Key in the database of TOEs. TOEs checks forgery and falsification, and assures the integrity of the transmitted digital signature. Also, it provides security features, such as access control, user data protection, and non-repudiation of origin (NRO).

Admin Portal (Hereafter; TOEa) provides audit data (UAF Operation history, user login history, admin history, etc.), and manages TOE license, Authenticator Metadata and SP information. Only authorized delivery manager, SP operation

[1] Authenticator: A FIDO UAF Authenticator is a secure entity, connected to or housed within FIDO user devices, that can create key material associated to a Relying Party. The key can then be used to participate in FIDO UAF strong authentication protocols.

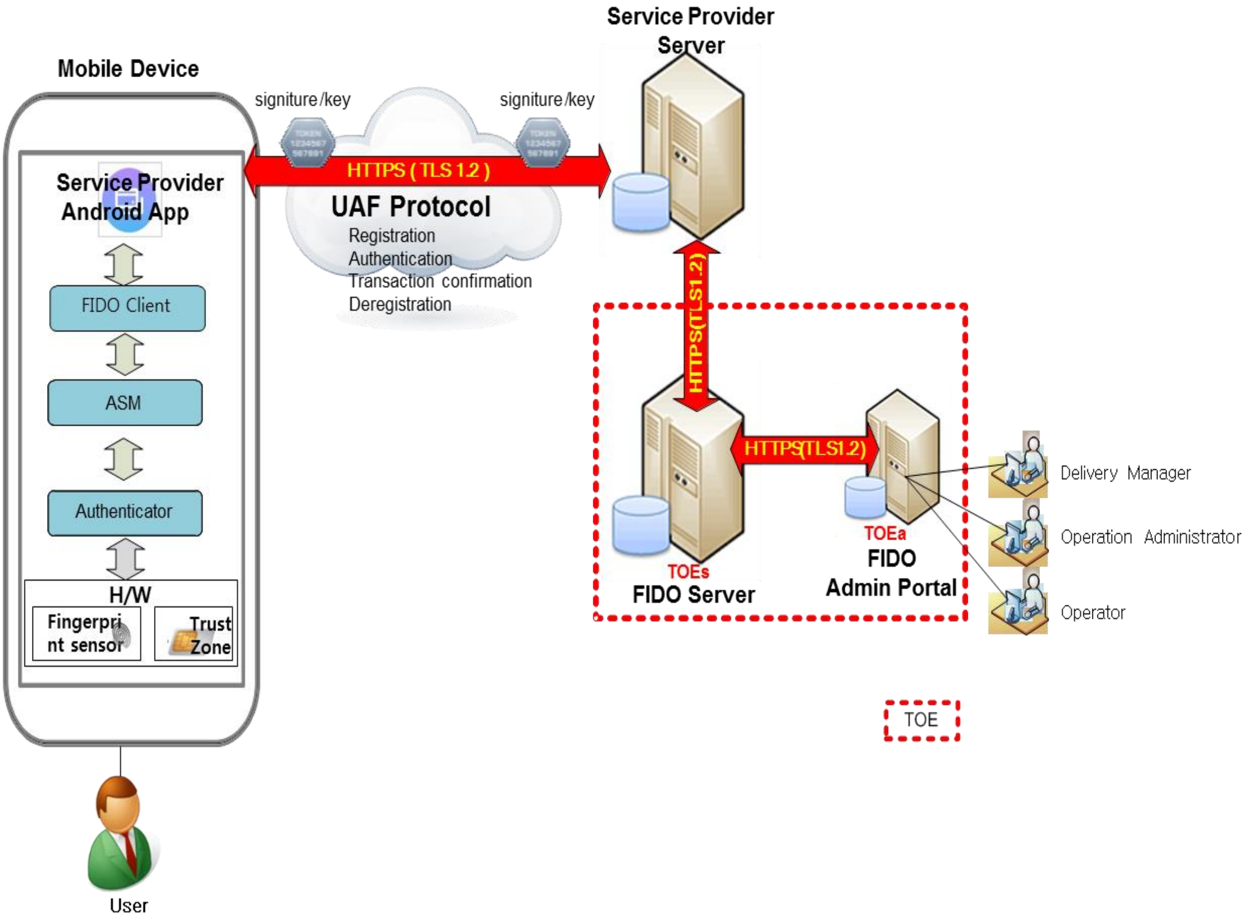
(Reference: https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-overview-v1.0-ps-20141208.html)

[2] FIDO Alliance: A non-profit organization formed in 2012 to address the global standard protocol and technical specification to use user's biometric information with members of Google, MS, Samsung Electronics, Master Card, etc.

administrator, and SP operator can use TOEa. TOE delivery manager register license, SP information, and Authenticator Metadata using TOEa. Operation administrator can register or modify license, Authenticator Metadata, SP information, and TOEa user information. Operation administrator and operator can access statistics data and audit data, such as UAF operation history, security warning, and admin history.

TOE Domain

TOE is composed of TOEs and TOEa.



Picture 1 TOE Operation Environment

Non-TOE Domain

FIDO Client, Authenticator, ASM, SP App, and SP Server are non-TOE Domain.
FIDO Client verifies if SP App is authorized and if there are Authenticators fit SP's policy, and handles interfaces between SP App and ASM.
Authenticator is a Secure Entity that is embedded in or housed within FIDO user devices. Authenticator generates user's public key and private key and signs a digital signature with private key and connected with ASM through Authenticator command.
ASM provides abstracted single API (ASM APIs) for compatibility between Authenticator and FIDO Client.
On service provider side, SP App and SP Server communicate based on HTTPS (TLS1.2) network environment. SP App is an application that is provided from Service Provider, for example, mobile Applications, such as mobile shopping App, mobile card App, mobile banking App. SP Server normally refers to application

of legacy Server. SP App and SP Server inter-connect through API based on UAF Protocol to communicate with FIDO Client and TOEs.

1.4 TOE Description

TOEs follows UAF Protocol, and it is the authentication system based PKI (PKI: Public Key Infrastructure)

TOEa verifies authorized administrators (delivery manager, SP operation administrator, and SP operator) and manages audit data by controlling access of SP data’s and Authenticator metadata‘s registration/modify/inquiry.

1.4.1 Required non-TOE Hardware/Software

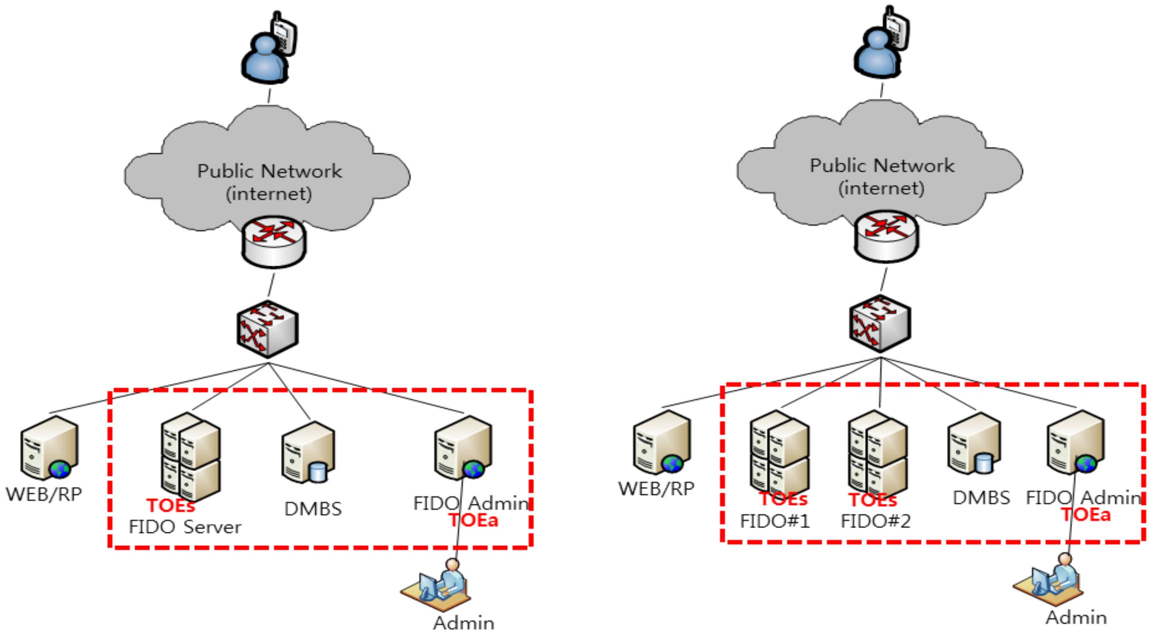
Hardware/Software specification required for TOE is described below, although it is not part of TOE.

Type	Category	OS	Minimum H/W Requirement				S/W
			CPU	MEM	NIC	HDD	
IDC	FIDO Server	Red Hat Enterprise Linux Server release 5.8	Intel Core i7 2.2GHz, 4Core	4GB RAM	10/100/1000 ethernet*1	320GB HDD	JDK 1.7
							nginx 1.8.0
							Redis 2.8.20
							Play Framework 2.3.2
	Admin Portal	Red Hat Enterprise Linux Server release 5.8	Intel Core i7 2.0GHz, 4Core	4GB RAM	10/100/1000 ethernet*1	320GB HDD	JDK 1.7
							nginx 1.8.0
							Anyframe Java 5.6.0 Community Ed.
							Apache Tomcat 7.0.59
							Third Party : aui library (Anyframe UI 1.0)
	DB Server	Red Hat Enterprise Linux Server release 5.8	Intel Core i7 2.0GHz, 4Core	4GB RAM	10/100/1000 ethernet*1	320GB HDD	MySQL 5.6.24
							Oracle 11g 11.2.0.1
	SP Server	Red Hat Enterprise Linux Server release 5.8	Intel Core i7 2.0GHz, 4Core	4GB RAM	10/100/1000 ethernet*1	320GB HDD	JDK 1.7
							nginx 1.8.0(TLS v1.2)
							Play Framework 2.3.2
	Admin Portal Console	Windows 7 Enterprise K (32bit/64bit)	PENTIUM 2.0 Ghz	1GB RAM	10/100/1000 ethernet*1	1GB HDD	Internet Explorer 11 Chrome 42.0.2311.90 m
Cloud	FIDO Server	Ubuntu 12.04 server Enterprise	Intel Xeon CPU X5670 Hexa 2.9GHz, 2Core	8GB RAM	Emulex 10G 2Port NIC * 2, Broadcom 1G * 4Port(On-B'd)	50GB HDD	JDK 1.7
							nginx 1.8.0
							Redis 2.8.20
							Play Framework 2.3.2
	Admin Portal	Ubuntu 12.04 server Enterprise	Intel Xeon CPU X5670 Hexa 2.9GHz, 2Core	4GB RAM	Emulex 10G 2Port NIC * 2, Broadcom 1G * 4Port(On-B'd)	50GB HDD	JDK 1.7
							Anyframe Java 5.6.0 Community Ed.
							Apache Tomcat 7.0.53
							Third Party : aui library (Anyframe UI 1.0)
	DB Server	Red Hat Enterprise Linux Server release 6.5	Intel Xeon CPU X5670 Hexa 2.9GHz, 2Core	16GB RAM	Emulex 10G 2Port NIC * 2, Broadcom 1G * 4Port(On-B'd)	140GB HDD	MySQL 5.6.20
							Oracle 11g 11.2.0.1
	SP Server	Ubuntu 12.04 server Enterprise	Intel Xeon CPU X5670 Hexa 2.9GHz, 2Core	4GB RAM	Emulex 10G 2Port NIC * 2, Broadcom 1G * 4Port(On-B'd)	50GB HDD	JDK 1.7
							nginx 1.8.0(TLS v1.2)
							Play Framework 2.3.2
	Admin Portal Console	Windows 7 Enterprise K (32bit/64bit)	PENTIUM 2.0 Ghz	1GB RAM	10/100/1000 ethernet*1	1GB HDD	Internet Explorer 11 Chrome 42.0.2311.90 m
GalaxyS 6(SM-G920) / GalaxyS 6 edge(SM-G925)	FIDO Client	Android 5.0	2.1GHz / 1.5GHz Octa-Core	3GB	N/A	32GB / 64GB(ROM)	Java 1.7
							Gson 2.2.4
							Guava 17.0
	ASM						N/A
	Authenticator						N/A

Table 1 Non-TOE Hardware/Software required in TOE

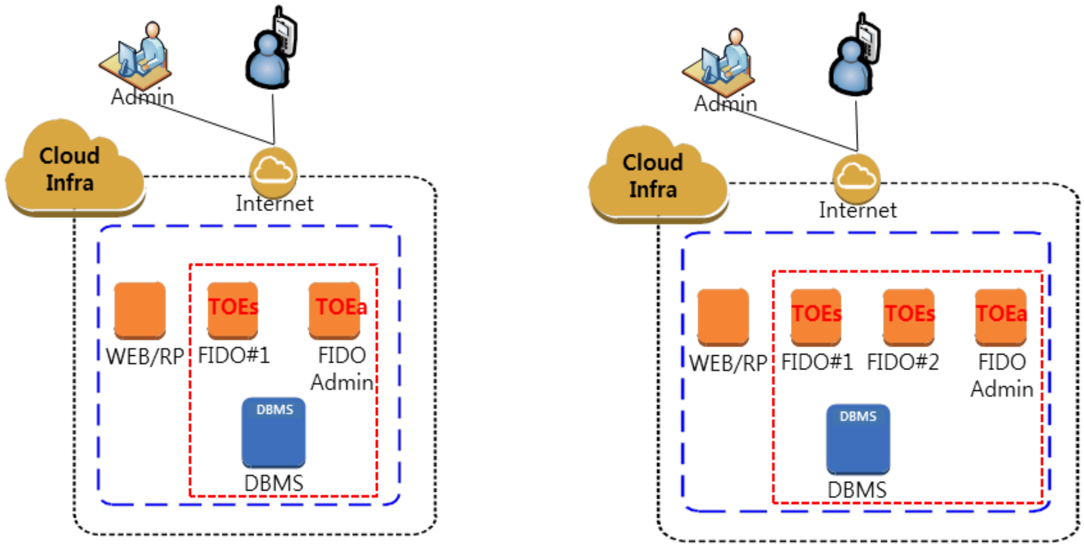
1.4.2 Physical scope of TOE

- IDC Environment



Picture 2 Physical Architecture of IDC environment

- Cloud Environment



Picture 3 Physical Architecture of Cloud environment

1.4.3 Logical scope of TOE

- TOEs Domain

TOEs consists of 9 subsystem, such as UAF, License Engine, Challenge Engine, Crypto Engine, Policy Engine, Trusted Facet Engine, Attestation Engine, RP Manager, Metadata Manager.

Main Security Feature

- FCS: Cryptographic Support
- FRN: Random Number
- FDP: User Data Protection
- FMT: Security management
- FPT: Protection of the TSF
- FCO: Communication

UAF (UAFS)
UAF, a sub-system called upon SP Server requests, executes subsequent process based on UAF Operation (Registration, Authentication, Transaction Confirmation, and Deregistration).

License Engine (LE)
License Engine verifies TOE's license so that only authorized SP Server can be access to the TOEs.

Challenge Engine (CES)
Challenge Engine generates the random bytes in the server challenge field contained in UAF Request Message and transmits it to FIDO Client. The server challenge is signed by Authenticator and contained in UAF Response Message. The UAF Response Message is transmitted to TOEs, and the TOEs verifies the server challenge and assures the integrity of UAF Response Message.

Crypto Engine (CE)
Crypto Engine is used when verifying digital signature with public key in registration, authentication, and transaction confirmation case. It is a sub-system in charge of cryptographic operation. It is used for assuring the integrity of digital signature generated by authenticator.

Policy Engine (PE)
Policy Engine constructs appropriate authentication policy of SP contained in UAF Request Message and transmitted to FIDO Client. When TOEs receives the UAF Response Message, PE can verify the policy if it does match the initial policy.

Trusted Facet Engine (TFE)
Trusted Facet Engine manages FacetList. When FIDO Client requests a FacetList, TFE sends it to FIDO Client. After UAF Response message is received, TFE verifies FacetID to detect if it is accessed through authorized SP App or not.

Attestation Engine (AE)
Attestation Engine assures the integrity of signed data generated by Authenticator.

RP[3] Manager (RM)

[3] RP is Relying Party, same as service provider.

RP Manager is called when authorized administrators (delivery manager/SP operation administrator/SP operator) of TOEa register or modify SP information (RP ID, API Key, App ID, FacetList, Policy, Etc.) through UI. RM checks if SP Server or TOEa is authorized by verifying API Key.

Metadata Manager (MM)
Metadata Manager is called when authorized administrators of TOEa register, modify, or delete Authenticator Metadata (AAID (Authenticator Attestation ID), Authenticator Version, Attestation Root Certificates, etc.) through UI or when verifying the digital signature.

- TOEa Domain

TOEa, as an audit of TOE, generates or searches audit data regarding security related issues. Only authorized administrators can register/modify/remove users, audit log in history, and control access to TOE assets by managing writing/changing rights for Authenticator Metadata and SP information.

Main Security Feature

- FIA: Identification & authentication
- FDP: User Data Protection
- FMT: Security management
- FAU: Security Audit

User Manager (UM)
User Manager manages menu and user role, manages data, such as TOEa user registration, modify, or remove, and provides log in/out features.

Log Manager (LM)
Log Manager generates audit history of TOE. Log Manager collects user log in history and admin activity history from TOEa.

License Manager (LSM)
License Manager can register/modify/remove Licenses.

UI (UI)
UI delivers input data from users to relevant sub-system.

Statistics Manager (SM)
Statistics Manager collects information from Log Manager, and reforms it as statistics.

1.5 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.
Section 2 of Conformance Claim claims conformance to Common Criteria, Protection Profile, and Package, and describes the rationale of conformance claims and the method of conformance by the security target.
Section 3 of Security problem Definitions describe the security problems of TOE and TOE operation environment from the perspectives of threats, organizational security policies, and assumptions.
Section 4 of Security Objectives describes the security objective for TOE and

the operation environment to countermeasure the threats identified in the security problem definitions, perform organizational security policies, and support assumptions.

Section 5 of Extended Component Definition identifies the extended security requirement of this security target and provides due explanation.

Section 6 contain 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.

Section 7 of TOE Summary Specification describes the TOE security function and assurance method satisfying TOE security requirements.

2 Conformance Claim

2.1 Common Criteria Conformance Claim

This security Target claims conformance to

- Common Criteria for Information Technology Security Evaluation, part 1: Instruction and general model, Version 3.1r4, September. 2012, CCMB-2012-09-001
- Common Criteria for Information Technology Security Evaluation, part 2: Security functional requirements, Version 3.1r4, September. 2012, CCMB-2012-09-002
- Common Criteria for Information Technology Security Evaluation, part 3: Security assurance requirements, Version 3.1r4, September. 2012, CCMB-2012-09-003

As follows

- Part 2 Extension
- Part 3 Conformant

2.2 Protection Profile Claim

This security Target does not conform to any Protection Profile.

2.3 Package Claim

This Security Target is conforming to assurance package as follows

- Assurance Package: EAL2 conformant

2.4 Preparation Rules

This security target uses English terms to clearly convey several meanings and acronyms. The used notation, shape, and preparation rules follow the common criteria of information protection system (Hereafter: common criteria)

Common Criteria allows repetition, allocation, selection and elaboration that can be performed in a security function requirement. Each operation is used in this security target.

Repetition
It is used when a component is repeated multiple times with various application of an operation. The result of a repetition operation is denoted with the repetition number in parentheses, as in (repetition number).

Assignment
The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are surrounded by square brackets as follows [assignment].

Selection
It is used to select on or more selection items provided by the common criteria for information protection system. The result of selection operation is denoted underlined and italicized.

Elaboration
It is used to limit the requirement further by adding details to the requirement. The result of an elaboration operation is denoted in bold

3 Security Problem Definition

Security problem Definition defines threats, organizational policy and assumptions that intended to be processed by TOE and TOE environment.

3.1 Threats

The threat agent is IT entities and human users to try the illegal access to the TOE or to threat the TOE with adverse action. It has the basic level of expertise, resources and motivation.

3.1.1 Threats from the device

T. Authenticator Duplication
The threat agent may damage the security of the TOE by disguising as an authorized authenticator with duplicated one.

T. ASM and FIDO Client Duplication
The threat agent may damage the security of the TOE by disguising as an ASM or a FIDO Client with duplicated ASM or FIDO Client.

T. Illegal Access
The threat agent may damage the security of the TOE and expose the user's data with the illegal access as disguised SP App, FIDO Client and ASM in the phase of the TOE operation.

3.1.2 Threats to the TOEs

T. Damage to Stored Data
The threat agent may expose, modify or delete TSF data and user data stored in the TOE with unauthorized way.

T. Illegal Access
The threat agent may damage the security of TOE and expose the user's data with the illegal access as disguised TOEa and SP Server in the phase of the TOE operation.

T. Replay Attack
The threat agent may replay the attack repetitively with the forged data after snatching the data between the device and the TOEs.

T. Transmitted Data Forgery
The threat agent may transmit the forged data after snatching the data between the device and the TOEs.

3.1.3 Threats to the TOEa

T. Consecutive Attempt to Authentication
The threat agent may acquire the authority of authorized administrator with consecutive attempt to authentication to access the TOE.

T. Damage to Stored Data
The threat agent may expose, modify or delete TSF data and user data stored in the TOE with unauthorized way.

3.2 Organizational Security Policies

The TOE shall comply with the organizational security policies specified in this chapter.

P. Audit
The TOEa shall record the security accidents precisely and maintain them securely to track the violated activities and shall audit the recorded data properly.

P. User Access Management
The TOEa shall provide the tool for the authorized user to manage the TSF data and user data securely.

User	Accessible Menu	Menu Description
SP Operator	Service History	Display the service history
	Statistics	Display the statistics
Delivery Manager / SP Operation Administrator	Service History	Display the service history
	Statistics	Display the statistics
	Master Data Management	Manage the metadata, SP and license
	System Management	Manage the history of user, administrator and login

Table 2 Menu Access by User

P. SP Development Guideline
It is required that SP App and SP Server be developed to use the FIDO functionalities in accordance with FIDO_Application Developer Manual (Client)_V1.1 and FIDO_Application Developer Manual (Server)_V1.1 delivered with the TOE.

P. Installation and Delivery
Delivery manager is required to install and deliver the TOE in accordance with installation manual.

3.3 Assumptions

The assumptions define the operation environment and operations of the TOE to limit the scope of security considerations.

A. Secured Storage

The secure element or trusted execution environment is provided for the authenticator to store the private key generated by the authenticator securely.

A. Robust Cryptography Algorithm

The authenticator uses robust cryptography algorithm when the authenticator generates the private and public key-pair and the signature to ensure the integrity

A. Secure Communication Channel

The TLS1.2 is used to ensure the confidentiality for the data transmission between SP APP and SP Server, and between TOEs and TOEa.

A. Protocol Compliance

The protocol defined in FIDO UAF Version 1.0(Framework (UAF) specs published on 2014-12-09) specification is complied with to communicate between SP App and SP Server.

A. Reliable Device Environment

The reliable SP App, FIDO Client, ASM and Authenticator are used in the device.

A. Trusted IT Environment

The TOE runs and operates securely in the trusted IT environment.

A. Timestamp

The reliable timestamp is provided in the TOE operation environment, SP.

A. DBMS

DBMS stores the TSF data and user data generated by the TOE securely, and operates the request by the authorized users.

4 Security Objectives

In this chapter, the security objectives are categorized into the TOE and operation environment. The security objectives of the TOE are directly handled by the TOE and the security objectives of the operation environment are handled by the technical and procedural method supported by the operation environment to provide the TOE security functionalities accurately.

4.1 Security Objectives for the TOE

The followings are the security objectives directly handled by the TOE.

O. Management

The TOE shall provide the method for the authorized manager to manage the TOE effectively.

O. Audit

The TOE shall record the security related activities accurately and maintain them securely to track the violated activities and shall audit the recorded data properly.

O. Identification and Authentication

The users shall be identified and authenticated to allow only authorized users to get the access to the TOE.

O. Access Control

The TOEs shall provide the access control functionalities to allow the authorized entity to get the access. The metadata and SP information, asset of the TOE shall be accessible for only authorized users (delivery manager, operation administrator) to register, modify and delete. In addition, the access from unauthorized TOEa or SP Server shall be controlled.

O. Transmitted Data Integrity

The authenticator shall create the signed data using private key and the signed data is transmitted to TOEs. When the TOEs receive the signed data, TOEs shall verify the integrity of the signed data.

4.2 Security Objectives for the Operation Environment

The followings are the security objectives handled by the technical and procedural method supported by the operation environment to provide the TOE security functionalities.

OE. Management

The TOE shall be delivered and installed securely and the authorized user of the TOE and the users of operation environment shall manage the TOE security.

OE. Secure Key Management

The authenticator shall store the private key in the secure storage such as secure element and trusted execution environment to protect the key from unauthorized access or exposure.

OE. Transmitted Data Integrity

The robust cryptography algorithm is used to ensure the integrity when the authenticator generates the private and public key-pair and the signed data.

OE. Transmitted Data Confidentiality

The TLS1.2 is used to ensure the confidentiality for the data transmission between SP APP and SP Server.

OE. Protocol Compliance
The protocol defined in FIDO UAF specification is complied with to communicate between SP App and SP Server, between SP App and FIDO Client, and between FIDO Client and ASM.

OE. Trusted IT Environment
The TOE runs and operates securely in the trusted IT environment.

OE. Reliable Device Environment
The reliable SP App, FIDO Client, ASM and authenticator are used in the device.

OE. Timestamp
The reliable timestamp is provided by SP, the TOE operation Environment.

OE. DBMS
DBMS stores the TSF data generated by the TOE securely, and operates the request by the authorized users.

4.3 Security Objectives Rationale

Security objectives rationale demonstrates that the specified security objectives are appropriate, sufficient to trace the security problems, and essential, rather than excessive.

The rationale of security objectives demonstrates the following:

- Each assumption, threat or organizational security policy is handled by at least one security objective.
- Each security objectives handles at least one assumption, threat or organizational security policy.

Table 3 shows the mapping between security problem definition and security objectives.

Security Objective / Security Problem Definition	Seurity Objectives					Security Environment								
	O.Management	O.Audit	O.Ident & Auth	O.Access Control	O.TDI	OE.Management	OE.SKM	OE.TDI	OE.TDC	OE.PC	OE.TIE	OE.RDE	OE.Timestamp	OE.DBMS
T. CAA			X											
T. Damage to Stored Data	X			X										
T. Replay Attack					X									
T. Transmitted Data Forgery					X									
T. Authenticator Duplication				X			X							
T. ASM & FIDO Client Duplication												X		
T. Illegal Access				X								X		
P. Audit		X												
P. SP Development Guideline										X				
P. Installation and Delivery	X					X								
P. User Access Managemnet	X			X										
A. Secure Storage							X							
A. Robust Cryptography Alg								X						
A. Protocol Compliance										X				
A. Secure CC									X					
A. Reliable Device Environment												X		
A. Trusted IT Environment											X			
A. Timestamp													X	
A. DBMS														X

Table 3 The mapping between Security Environment and Security Objectives

※ CAA : Consecutive Attempt Authentication

※ Iden & Auth : Identification & Authentication

※ TDI : Transmitted Data Integrity

※ SKM : Secure Key Management

※ TDC : Transmitted Data Confidentiality

※ PC : Protocol Compliance

※ TIE : Trusted IT Environment

※ RDE : Reliable Device Environment

Security Problem	Security Objective to be Mapped	Theoretical Basis
T. Consecutive Attempt to Authentication	O. Identification and Authentication	O. Identification and Authentication: Since the TOEa provides the access to delivery manager, operation administrator and operator before starting the security management operation and TOEa can't be accessed after five consecutive authentication failures, it takes action against T. Consecutive Attempt To Authentication.
T. Damage to Stored Data	O. Access Control O. Management	O. Access Control: Since the TOE prevents modifying the data through the unauthorized access and is accessible for only authorized users to register, modify and delete the data on installing the TOE, it takes action against T. Damage to Stored Data. O. Management: Since the way to the TSF data and user data managed securely by the TOE is provided, it takes action against T. Damage to Store Data.
T. Replay Attack	O. Transmitted Data Integrity	O. Transmitted Data Integrity: Since the TOEs takes the following steps to verify the data integrity and to sense the data forgery by the unauthorized entity, it takes action against T. Replay Attack. (1) TOEs generates the random number and transmits it to the authenticator which is the TOE operation environment (2) The authenticator signs the random number with private key and transmit it back to the TOEs (3) TOEs compares the number received with the original generated number after verifying it with public key
T. Transmitted Data Forgery	O. Transmitted Data Integrity	O. Transmitted Data Integrity: Since the authenticator, the TOE operation environment transmits the signed data with the private key to the TOEs, and then the TOEs verifies it with the public key to ensure the data integrity, it takes action against T. Transmitted Data Forgery.
T. Authenticator Duplication	O. Access Control OE. Secured Key Management	O. Access Control: Since the authenticator, the TOE operation environment increases the number for succeeded authentication and transmits this number to TOEs DB to compare it with the stored number and to confirm the device is not duplicated; it takes action against T. Authenticator Duplication. OE. Secured Key Management: Since the authenticator stores the private key in the secure storage such as Secure Element and Trusted Execution Environment and ensures the security from the unauthorized access or exposure to it, it takes action against T. Authenticator Duplication.

T. ASM and FIDO Client Duplication	OE. Reliable Device Environment	OE. Reliable Device Environment Since the inter-accessibility is allowed only in the case that FIDO Client and ASM use the same private key in Android Platform, it is impossible for the duplicated application to have an access. Since the device manufacturer ensures the reliable device environment by pre-embedding FIDO Client and ASM with the signature with same private key, it takes action against T. ASM and FIDO Client Duplication.
T. Illegal Access	O. Access Control OE. Reliable Device Environment	O. Access Control (TOEs) Since the TOEs assigns the unique key(API Key) to SP Server on installation and identifies it when SP Server accesses the TOEs to control the access by the unauthorized SP Server, it takes action against T. Illegal Access. Since the TOEs assigns the unique key(API Key) to TOEa on installation and identifies it when TOEa accesses the TOEs to control the access by the unauthorized TOEa, it takes action against T. Illegal Access. OE. Reliable Device Environment(SP App, FIDO Client, ASM) Since SP App signed by SP is installed in the device to verify the disguised SP App with FacetID when it tries illegal access to FIDO Client, it takes action against T. Illegal Access. Since the inter-accessibility is allowed only in the case that FIDO Client and ASM use the same private key in Android Platform, it is impossible for the duplicated application to have an access. Since the device manufacturer ensures the reliable device environment by pre-embedding FIDO Client and ASM with the signature with same private key, it takes action against T. ASM and FIDO Client Duplication.
P. Audit	O. Audit	O. Audit: Since the TOE records the security audit data from the security related accidents and provides the method to manage/review it, it takes action for P. Audit.
P. SP Development Guideline	OE. Protocol Compliance	OE. Protocol Compliance: Since SP App and SP Server are developed to use the FIDO functionalities in accordance with FIDO_Application Developer Manual (Client)_V1.1 and FIDO_Application Developer Manual (Server)_V1.1, it takes action for P. SP Development Guideline.
P. Delivery	O. Management OE. Management	O. Management & OE. Management: Since the TOE is delivered and installed securely and is configured and managed by the authorized users for the TOE and TOE operation environment, it takes action for P. Delivery.

P. User Access Management	O. Access Control O. Management	O. Access Control: Since the TOEs prevents modifying the data through the unauthorized access and is accessible for only authorized users to register, modify and delete the data on installing the TOEs, it takes action for P. User Access Management. O. Management: Since the TOE is delivered and installed securely and ensures the only authorized user stores and manages the data, it takes action for P. User Access Management.
A. Secured Storage	OE. Secured Key Management	OE. Secured Key Management: Since the authenticator stores the private key in the secure storage such as Secure Element and Trusted Execution Environment and ensures the security from the unauthorized access or exposure to it, it takes action for A. Secured Storage.
A. Robust Cryptography Algorithm	OE. Transmitted Data Integrity	OE. Transmitted Data Integrity: Since the authenticator uses robust cryptography algorithm when the authenticator generates the private and public key-pair and the signature to ensure the integrity, it takes action for A. Robust Cryptography Algorithm.
A. Protocol Compliance	OE. Protocol Compliance	OE. Protocol Compliance: Since the UAF protocol is complied with to communicate between SP App and SP server, between SP App and FIDO Client, and between FIDO Client and ASM, it takes action for A. Protocol Compliance.
A. Secure Communication Channel	OE. Transmitted Data Confidentiality	OE. Transmitted Data Confidentiality: Since the TLS1.2 is used to ensure the confidentiality for the data transmission between SP APP and SP Server, it takes action for A. Secure Communication Channel.
A. Reliable Device Environment	OE. Reliable Device Environment	OE. Reliable Device Environment: Since the reliable SP App, FIDO Client, ASM and Authenticator are used in the device, it takes action for A. Reliable Device Environment.
A. Trusted IT Environment	OE. Trusted IT Environment	OE. Trusted IT Environment: Since the TOE runs and operates securely in the trusted IT environment, it takes action for A. Trusted IT Environment.
A. Timestamp	OE. Timestamp	OE. Timestamp: Since the reliable timestamp is provided by SP, the TOE operation Environment, it takes action for A. Timestamp.
A.DBMS	OE.DBMS	OE. DBMS: Since DBMS stores the TSF data generated by the TOE securely and operates the request by the authorized users, it takes action for A. DBMS.

Table 4 Security Problem Definition and Security Objectives Action / Theoretical Basis

5 Definition of Extended component (ASE_ECD)

This chapter identifies the extended security requirement along with Part 2 of common criteria and the following [Table 5] shows the extended components of security requirements.

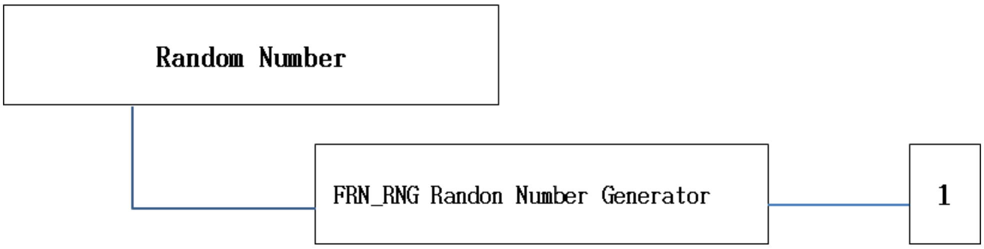
- FRN_RNG.1(Extended) Random Number Generator

Security Functional Class	Security Functional Component	
Random Number	**FRN_RNG.1(Extended)**	Random Number Generator

Table 5 Random number class composition

5.1 Random Number Class

Random number class specifies the random number creation feature with robust algorithm. FRN class is composed of a family FRN_RNG.



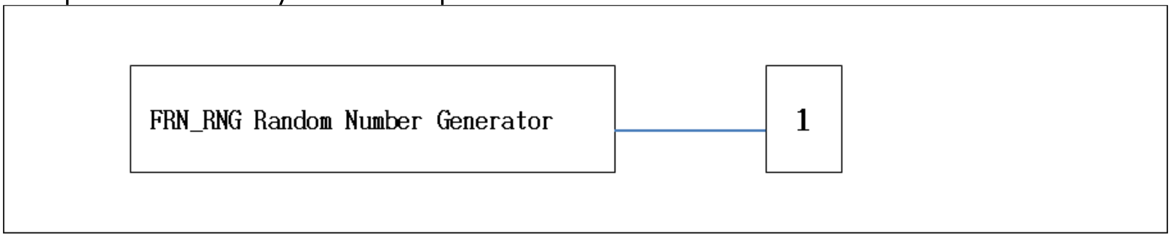
Picture 4 Random number class component

5.1.1 Random Number Generator

Family overview

Random number creation (FRN_RNG) family prevents the replay attack and defines requirements of number creation method to verify the signature.

Component hierarchy and description



Picture 5 Random number creation components and hierarchy

FRN_RNG.1 Generation of random numbers requires that random numbers meet a defined quality metric.
There are no management activities foreseen.
There are no actions defined to be auditable.

FRN_RNG.1 Random number generation
Hierarchical to : No other components
Dependencies : No dependencies

FRN_RNG.1.1 The TSF shall provide a *selection : physical, non-physical true, deterministic, pseudo, hybrid* random number generator that implements

FRN_RNG.1.2 The TSF shall provide random numbers that meet [assignment : a defined quality metric]

6 Security functional requirements

6.1 TOE Security functional requirements

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 2 providing assurance requirements

The security functional requirements are expressed using the notation stated in Section 2.4 above and itemized in the table below.

Security Functional Class	Level	Functional Family	Security objectives
FCS: Cryptographic Support	FCS_COP.1	FCS_COP, Cryptographic operation	O. Transmitted Data Integrity
FRN: Random Number	FRN_RNG.1	FRN_RNG, Random Numer Generation	O. Transmitted Data Integrity
FDP: User Data Protection	FDP_ACC.1(1)	FDP_ACC, Access control Policy	O. Access Control
	FDP_ACF.1(1)	FDP_ACF, Access control functions	O. Access Control
	FDP_ACC.1(2)	FDP_ACC, Access control Policy	O. Access Control
	FDP_ACF.1(2)	FDP_ACF, Access control functions	O. Access Control
FIA, Identification & authentication	FIA_AFL.1	FIA_AFL, Authentication failures	O. Identification & authentication
	FIA_SOS.1	FIA_SOS, Specification of secrets	O. Identification & authentication
	FIA_UAU.7	FIA_UAU, User authentication	O. Identification & authentication
	FIA_UAU.2	FIA_UAU, User authentication	O. Identification & authentication
	FIA_UID.2	FIA_UID, User identification	O. Identification & authentication
FMT, Security management	FMT_MOF.1	FMT_MOF, Management of function in TSF	O. Management
	FMT_MSA.1	FMT_MSA, Management of security attributes	O. Management
	FMT_MSA.3	FMT_MSA, Management of security attributes	O. Management
	FMT_SMF.1	FMT_SMF, Specification of Management Functions	O. Management
	FMT_SMR.1	FMT_SMR, Security management roles	O. Management
FPT, Protection of the TSF	FPT_TDC.1	FPT_TDC, Inter-TSF TSF data consistency	O. Transmitted Data Integrity
FAU, Security Audit	FAU_ARP.1	FAU_ARP, Security audit automatic response	O. Audit
	FAU_GEN.1	FAU_GEN, Security audit data generation	O. Audit
	FAU_GEN.2	FAU_GEN, Security audit data generation	O. Audit

	FAU_SAR.1	FAU_SAR, Security audit review	O. Audit
	FAU_SAR.3	FAU_SAR, Security audit review	O. Audit
	FAU_SAA.1	FAU_SAA, Security audit analysis	O. Audit
FCO, Communication	FCO_NRO.1	FCO_NRO, Non-repudiation of origin	O. Transmitted Data Integrity

Table 6 TOE Security Functional Requirements

External IT entity

- SP Server
- DB Server
- Mobile device user

6.1.1 Cryptographic Support

FCS_COP.1 Cryptographic operation(Digital Signature Verification)

Hierarchical to : No other components

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

FCS_COP.1.1 The TSF shall perform [Digital signature verification] in accordance with a specified cryptographic algorithm [Signature algorithm of table 7] and cryptographic key sizes [Cryptographic key sizes of table 7] that meet the following : [List of standards of Table 7]

List of standards	Signature Algorithm	Cryptographic key sizes	Description
ECDSA Signature ANSI X9.62-2005	SECP256R1_ECDSA_SHA256_RAW	256bit	An ECDSA signature on the NIST secp256r1 curve which MUST have raw R and S buffers, encoded in big-endian order. I.e. [R (32 bytes), S (32 bytes)]
	SECP256R1_ECDSA_SHA256_DER	256bit	DER [ITU-X690-2008] encoded ECDSA signature [RFC5480] on the NIST secp256r1 curve. I.e. a DER encoded SEQUENCE { r INTEGER, s INTEGER }
	SECP256K1_ECDSA_SHA256_RAW	256bit	An ECDSA signature on the secp256k1 curve which MUST have raw R and S buffers, encoded in big-endian order. I.e.[R (32 bytes), S (32 bytes)]
	SECP256K1_ECDSA_SHA256_DER	256bit	DER [ITU-X690-2008] encoded ECDSA signature [RFC5480] on the secp256k1 curve. I.e. a DER encoded SEQUENCE { r INTEGER, s INTEGER }

RSASSA-PSS signature [RFC3447], [RFC4055], [RFC4056]	RSASSA_PSS_SHA256_RAW	256bit	RSASSA-PSS [RFC3447] signature MUST have raw S buffers, encoded in big-endian order [RFC4055] [RFC4056]. The default parameters as specified in [RFC4055] MUST be assumed, i.e. •Mask Generation Algorithm MGF1 with SHA256 •Salt Length of 32 bytes, i.e. the length of a SHA256 hash value. •Trailer Field value of 1, which represents the trailer field with hexadecimal value 0xBC. I.e. [S (256 bytes)]
	RSASSA_PSS_SHA256_DER	256bit	DER [ITU-X690-2008] encoded OCTET STRING (not BIT STRING!) containing the RSASSA-PSS [RFC3447] signature [RFC4055] [RFC4056]. The default parameters as specified in [RFC4055] MUST be assumed, i.e. •Mask Generation Algorithm MGF1 with SHA256 •Salt Length of 32 bytes, i.e. the length of a SHA256 hash value. •Trailer Field value of 1, which represents the trailer field with hexadecimal value 0xBC. I.e. a DER encoded OCTET STRING (including its tag and length bytes).

Table 7 Digital Signature Algorithm [4]

※ TOEs perform Digital signature verification in accordance with a specified signature algorithm of table 7. But the Authenticator of Galaxy S6(SM-G920) or Galaxy S6 edge(SM-G925) creates digital signature only with SECP256R1_ECDSA_SHA256_RAW

6.1.2 Random number generation

FRN_RNG.1 Random number generation

Hierarchical to: No other components
Dependencies: No dependencies

FRN_RNG.1.1 The TSF shall provide a *pseudo* random number generator.

FRN_RNG.1.2 The TSF shall provide random numbers that meet [RFC1750:Randomness Recommendations for Security]

6.1.3 User Data Protection

FDP_ACC.1(1) Subset access control

Hierarchical to: No other components
Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [SFP of table 8] on [list of subjects, object and operations among subjects and objects covered by the SFP of table 8].

SFP	Subject	Subjects Security Attribute	Object	Objects Security Attribute	Operations
SP Server	IT entity using SP	API Key	TOEs	API Key	TOEs Access

Access Control	Server				Permission
Authenticator Access Control	IT entity using Authenticator	Signature Counter	TOEs	Signature Counter	TOEs Access Permission
TOEa Access Control	IT entity using TOEa	API Key	TOEs	API Key	TOEs Access Permission

Table 8 Operation for Subject & Object

Detailed Security Attribute	Access Control Rule	Access Authorization Rule	Access Denial Rule
API Key	To verify that the API Key of SP server is identical to the API Key stored on TOEs	SP Server is allowed to access TOEs when the API Key matches	SP Server is denied to access TOEs when API Key does not match
Signature Counter	To compare Authenticator's Signature Counter to TOEs' Signature Counter	TOEs is allowed to access if Authenticator's Signature counter is greater than TOEs' Signature counter	TOEs is denied to access if Authenticator's Signature counter is the same or smaller than TOEs' Signature counter
API Key	To verify that the API Key of Admin Portal server is identical to the API Key saved on TOEs	TOEa is allowed to access TOEs when the API Key does match	TOEa is denied to access TOEs when API Key does not match

Table 9 Access Rule by Detailed Security Attributes

FDP_ACF.1(1) Security attribute based access control
Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [SFR of table 8] to objects based on the following : [Table 8]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:[Table 9]

FDP_ACF.1.3 The TSF shall explicitly authorize 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]

FDP_ACC.1(2) Subset access control
Hierarchical to : No other components
Dependencies : FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [SFP of table 11] on [assignment : list of subjects, object and all operations among subjects and objects covered by the SFP of table 11].

Menu	List of information	Function

Master Data Management	Authenticator Meta	Add, modify, inquire
	Service Provider Information	Add, modify, inquire
System Management	User Information	Add, modify, delete, inquire
	Admin History, Login History	Inquire

Table 10 Functions by Information

SFP	Subject	Subject security attribute	Object	Object security attribute	Operation
Security Data Access Control	Operator	Users	Master Data Management, System Management	Deactivation	Permission to add, modify, delete, inquire
	Delivery Manager	Administrators	Master Data Management, System Management	Activation	Permission to add, modify, delete, inquire
	Operation Administrator	Administrators	Master Data Management, System Management	Activation	Permission to add, modify, delete, inquire

Table 11 Operation by Subject & Object

Detailed Security Attribute	Access control Rule	Access Authorization Rule	Access denial Rule
Users	Operator is not allow to access to the Master Data Management, System Management menu because the operator has 'Users' security attributes	N/A	If detail security attribute is 'Users', access to Master Data Management and System Management menu is denied
Administrators	Delivery Manager and Operation Administrator is allowed to add, modify and delete Master Data Management, System Management menu	When detailed security attribute is 'Administrators', Master Data Management and System Management menu is accessible	N/A

	because they have 'Administrators' security attributes		

Table 12 Access Rule by detailed security attributes

FDP_ACF.1(2) Security attribute based access control
Hierarchical to: No other components
Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialization

FDP_ACF.1.1 The TSF shall enforce the [SFP of Table 11] to objects based on the following: [Table 11]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:[Table 12]

FDP_ACF.1.3 The TSF shall explicitly authorize 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]

6.1.4 Identification and authentication

FIA_AFL.1 Authentication failure handling (TOEa)
Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_AFL.1.1 The TSF shall detect when *an administrator configurable positive integer within [5]* unsuccessful authentication attempts occur related to [authentication of TOEa user]
FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been *met* the TSF shall [lock user account].

FIA_SOS.1 Verification of secrets
Hierarchical to: No other components
Dependencies: No dependencies

FIA_SOS1.1 The TSF shall provide a mechanism to verify that secrets meet [Table 13].

Security Attributes	Description
Length	Min8 ~ Max 20 characters in length
Character type	• a-z (26) • A-Z (26) • 0-9 (10) • Special characters (32) : ~ ! @ # $ % ^ * ( ) _ + | `- = \ { } : ” < > ? [ ] ; ’ , . / “
Rule for password	Contain 3/4 of the following items: Uppercase Letters, Lowercase Letters, Numbers, special characters.
note	Replace password with “*”

Table 13 Security Attribute of secrets

FIA_UAU.2 User authentication before any action (TOEa)

Hierarchical to: FIA_UAU.1 Timing of authentication
Dependencies: FIA_UID.1 Timing of identification

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.

FIA_UAU.7 Protected authentication feedback (TOEa)

Hierarchical to: No other components
Dependencies: FIA_UAU.1 Timing of authentication

FIA_UAU.7.1 The TSF shall provide only [*] to the user while the authentication is in progress.

FIA_UID.2 User identification before any action (TOEa)

Hierarchical to: FIA_UID.1 Timing of identification
Dependencies: No dependencies

FIA_UID.2.1 The shall require each user to be successfully identified before allowing any other TSF-mediated action on behalf of that user..

6.1.5 Management of functions in TSF

FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components
Dependencies: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

The TSF shall restrict the ability *to determine the behavior of* the functions [list of functions of Table 14] to [the authorized roles of Table 14]

List of functions	Authorized Roles
Add, Modify, Inquire Authenticator Meta	Delivery Manager, Operation Administrator
Add, Modify, Inquire Service Provider Info	
Add , Modify, Inquire User Info	
Inquire Admin History Inquire Login History	
Activation, Deactivation of User Account	
Delete, Inquire Security Warning	Operation Administrator, Operator
Add, Delete, Inquire BlackList	
Add API Key of TOEa	Delivery Manager

Table 14 Function by Authorized Roles

FMT_MSA.1 Management of security attribute

Hierarchical to: No other components
Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

Security Attributes	Detailed Security Attribute	Action	Authorized Role
GroupName	Users	select	Delivery Manager, SP Operation Administrator
	Administrators		
API Key(SP Server의)	N/A	Initialization, Query, Register, Modify	Delivery Manager, SP Operation Administrator

Table 15 Security Attributes-Action by Authorized Role

FMT_MSA.1.1 The TSF shall enforce the [SFP of Table 8 and Table 11] to restrict the ability to *[Action of Table 15]* the security attribute [security attributes of Table 15] to [the authorized roles of Table 15].

FMT_MSA.3 Static attribute initialization
Hierarchical to: No other components
Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [SFP(s) of FDP_ACC.1(1), FDP_ACC.1(2)] to Provide *restrictive* default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [Delivery manager, SP Operation Administrator] to specify alternative initial values to override the default values when an object or information is created

FMT_SMF.1 Specification of Management Functions
Hierarchical to: No other components
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [list of management functions of Table 14]

FMT_SMR.1 Security roles
Hierarchical to: No other components
Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles [Delivery manager, SP Operation Administrator, SP Operator].

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

6.1.6 Protection of the TSF

FPT_TDC.1 Inter-TSF basic TSF data consistency
Hierarchical to: No other components
Dependencies: No dependencies

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [UAF Message specified in FIDO UAF protocol specification] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [FIDO UAF protocol specification] when interpreting the TSF data from another trusted IT product.

6.1.7 Security Audit

FAU_ARP.1 Security alarms
Hierarchical to: No other components
Dependencies: FAU_SAA.1 Potential violation analysis

FAU_ARP.1.1 The TSF shall take [steps below] upon detection of a potential security violation.

a) Store error history in DB(logging_event Table)
b) Run Batch and Check if there is any violation noted in table 17.
c) If there is, add the violation in Security warning table.

FAU_GEN.1 Audit data generation
Hierarchical to : No other components
Dependencies : FPT_STM.1 Reliable time stamps

FAU_GEN1.1 The TSF shall be able to generate an audit record of the following auditable events.

a) Start-up and shutdown of the audit functions;
b) All auditable events for the *not specified* level of audit; and
c) [the auditable events of Table 16]

SFRs	Audit data
FIA_AFL.1	Identification/Authentication failure history of administrator
FIA_UAU.2	Identification/Authentication success / failure history of administrator
FIA_UID.2	Identification/Authentication success / failure history of administrator
FMT_MOF.1	TSF data management history by administrator
FCO_NRO.1	Digital Signature Verification failure history
FAU_ARP.1	Security Warning history

Table 16 Audit Event

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information

a) Data and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the events: and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [none]

FAU_GEN.2 User identity association
Hierarchical to: No other components
Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

FAU_SAA.1 Potential violation analysis
Hierarchical to: No other components
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the enforcement of the SFRs.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of [subset of defined auditable events of Table 17] known to indicate a potential security violation;

b) [none]

NO	Operation	Potential violation analysis list
1	Registration	RegAssertion decoding failed
2		Assertion Scheme mismatch
3		Not support Attestation type
4		Attestation type mismatch
5		Final Challenge Hash mismatch
6		Authenticator version mismatch
7		Limitation value excess RegCounter
8		Root Certificate does not exist
9		Digital Signature verification failure
10	Authentication	SignAssertion decoding failed
11		Assertion Scheme mismatch
12		Authenticator version mismatch
13		UserID mismatch
14		Sign Counter does not increase
15		Not support Attestation type
16		Final Challenge Hash mismatch
17		Authentication mode mismatch
18		Transaction is not found for Transaction confirmation
19		Transaction is found for Non-Transaction confirmation
20		Digital Signature verification failure

Table 17 list of Potential violation

FAU_SAR.1 Audit review
Hierarchical to: No other components
Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.1.1 The shall provide [Delivery Manager, Operation Administrator] with the capability to read [list of audit information of TOEa] from the audit records.
FAU_SAR1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information

FAU_SAR.3 Selectable audit review
Hierarchical to: No other components
Dependencies: FAU_SAR.1 Audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply [Search Element of TOEa] of audit data based on [Search, Sort]

a) Search

: RequestID, Request Type, UserID, Service Provider, Result, Status Code, Period, LicenseID, Service IP, Customer Name, Authenticator, API Key, APP ID, Report Type

b) Sort : Sort out by timeline (Default 10 rows)

6.1.8 Non-repudiation of origin

FCO_NRO.1 Selective proof of origin

Hierarchical to: No other components

Dependencies: FIA_UID.1 Timing of identification

FCO_NRO.1.1 The TSF shall be able to generate evidence of for transmitted [Registration, Authentication, Transaction Confirmation] at the request of the *[Mobile Device User, Service Provider]*.

FCO_NRO.1.2 The TSF shall be able to relate the [Key Registration Data, Signed Data] of the originator of the information, and the [Key Registration Data, Signed Data] 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 *[Mobile Device User, Service Provider]* given [The digital signature is generated by Authenticator with private key]

Key Registration Data	Description
AAID	Authenticator Attestation ID
AuthenticatorVersion	Vendor assigned authenticator version
AuthenticationMode	Registration or Authentication
SignatureAlgAndEncoding	Signature Algorithm and Encoding of attestation signature
PublicKeyAlgEndEncoding	Public Key algorithm and encoding of the newly generated Uauth.pub key
FinalChallenge	Final Challenge
KeyID	KeyID generated by Authenticator
SignCounter	Indicates how many times this authenticator has performed signatures in the past.
RegCounter	Indicates how many times this authenticator has performed registrations in the past.
PublicKey	User Authentication public key(Uauth.pub) newly generated by authenticator
signature	Signature calculated with Basic Attestation Private Key over TAG_UAFV1_KRD content. The entire TAG_UAFV1_KRD content, including the tag and it's length field, must be included during signature computation.

Certificate	Single X.509 DER-encoded [ITU-X690-2008] Attestation Certificate or a single certificate from the attestation certificate chain (see description above).

Table 18 Key Registration Data[5]

Signed Data	Description
AAID	Authenticator Attestation ID
AuthenticatorVersion	Vendor assigned authenticator version
AuthenticationMode	Registration or Authentication
SignatureAlgAndEncoding	Signature Algorithm and Encoding format
FinalChallenge	Final Challenge
TCHash	(binary value of) Transaction Content Hash
KeyID	KeyID generated by Authenticator
SignCounter	Indicates how many times this authenticator has performed signatures in the past.
signature	Signature calculated using UAuth.priv over TAG_UAFV1_SIGNED_DATA structure. The entire TAG_UAFV1_SIGNED_DATA content, including the tag and it's length field, must be included during signature computation.

Table 19 Signed Data[5]

6.2 TOE Security Assurance Requirements

The security assurance requirement for this Security Target consist of the following components from Part 3 of the CC, summarized in the following [Table 20 Assurance Requirement] and evaluation assurance level is EAL2.

In this Security Target, the assurance components are summarized as follows:

Assurance class	Assurance components	
ASE: Security Target evaluation	ASE_INT.1	ST Instruction
	ASE_CCL.1	Conformance claims
	ASE_SPD.1	Security Problem Definition
	ASE_OBJ.2	Security objectives
	ASE_ECD.1	Extended components definition
	ASE_REQ.2	Derived security requirements
	ASE_TSS.1	TOE summary specification
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance documents	AGD_OPE.1	Operational user guidance

	AGD_PRE.1	Preparative procedures
Life cycle support	ALC_CMC.2	Use of a CM system
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

Table 20 Security Assurance Requirements

6.2.1 Security target evaluation

ASE_INT.1 ST introduction

Dependencies: No dependencies.

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

ASE_INT.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

ASE_CCL.1 Conformance claims

Dependencies:

ASE_INT.1 ST introduction

ASE_ECD.1 Extended components definition

ASE_REQ.1 Stated security requirements

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.
ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.
ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.
ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.
ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.
ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.
ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

Evaluator action elements:

ASE_CCL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_SPD.1 Security problem definition

Dependencies: No dependencies.

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.
ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.
ASE_SPD.1.3C The security problem definition shall describe the OSPs.
ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

ASE_SPD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_OBJ.2 Security objectives

Dependencies:

ASE_SPD.1 Security problem definition

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.
ASE_OBJ.2.2D The developer shall provide a security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.
ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.
ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1 Extended components definition

Dependencies: No dependencies.

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

ASE_ECD.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

ASE_REQ.2 Derived security requirements

Dependencies:

ASE_OBJ.2 Security objectives

ASE_ECD.1 Extended components definition

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirements rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1 TOE summary specification

Dependencies:

ASE_INT.1 ST introduction

ASE_REQ.1 Stated security requirements

ADV_FSP.1 Basic functional specification

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

Content and presentation elements:

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

ASE_TSS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification

6.2.2 Development

ADV_ARC.1 Security architecture description

Dependencies:

ADV_FSP.1 Basic functional specification

ADV_TDS.1 Basic design

Developer action elements:

ADV_ARC.1.1D The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2D The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3D The developer shall provide a security architecture description of the TSF.

Content and presentation elements:

ADV_ARC.1.1C The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2C The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3C The security architecture description shall describe how the TSF initialization process is secure.

ADV_ARC.1.4C The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5C The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

Evaluator action elements:

ADV_ARC.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2 Security-enforcing functional specification

Dependencies:

ADV_TDS.1 Basic design

Developer action elements:

ADV_FSP.2.1D The developer shall provide a functional specification.

ADV_FSP.2.2D The developer shall provide a tracing from the functional specification to the SFRs.

Content and presentation elements:

ADV_FSP.2.1C The functional specification shall completely represent the TSF.

Class ADV: Development September 2012 Version 3.1 Page 91 of 233

ADV_FSP.2.2C The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3C The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4C For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5C For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_FSP.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_FSP.2.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

ADV_TDS.1 Basic design

Dependencies:

ADV_FSP.2 Security-enforcing functional specification

Developer action elements:

ADV_TDS.1.1D The developer shall provide the design of the TOE.

ADV_TDS.1.2D The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.

Content and presentation elements:

ADV_TDS.1.1C The design shall describe the structure of the TOE in terms of subsystems.

ADV_TDS.1.2C The design shall identify all subsystems of the TSF.

ADV_TDS.1.3C The design shall describe the behaviour of each SFR-supporting or SFR non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.

ADV_TDS.1.4C The design shall summarize the SFR-enforcing behaviour of the SFR enforcing subsystems.

ADV_TDS.1.5C The design shall provide a description of the interactions among SFR enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.

ADV_TDS.1.6C The mapping shall demonstrate that all TSFIs trace to the behavior described in the TOE design that they invoke.

Evaluator action elements:

ADV_TDS.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_TDS.1.2E The evaluator shall determine that the design is an accurate.

6.2.3 Guidance documents

AGD_OPE.1 Operational user guidance

Dependencies:

ADV_FSP.1 Basic functional specification

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

AGD_OPE.1.1E The evaluator shall confirm that the information provided

AGD_PRE.1 Preparative procedures

Dependencies: No dependencies.

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Content and presentation elements:

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

AGD_PRE.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AGD_PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation

6.2.4 Life-cycle support

ALC_CMC.2 Use of a CM system

Dependencies:

ALC_CMS.1 TOE CM coverage

Developer action elements:

ALC_CMC.2.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.2.2D The developer shall provide the CM documentation.
ALC_CMC.2.3D The developer shall use a CM system.

Content and presentation elements:

ALC_CMC.2.1C The TOE shall be labelled with its unique reference.
ALC_CMC.2.2C The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3C The CM system shall uniquely identify all configuration items.

Evaluator action elements:

ALC_CMC.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_CMS.2 Parts of the TOE CM coverage

Dependencies: No dependencies

Developer action elements:

ALC_CMS.2.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.2.1C The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2C The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3C For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.

Evaluator action elements:

ALC_CMS.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ALC_DEL.1 Delivery procedures

Dependencies: No dependencies.

Developer action elements:

ALC_DEL.1.1D The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2D The developer shall use the delivery procedures.

Content and presentation elements:

ALC_DEL.1.1C The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.

Evaluator action elements:

ALC_DEL.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.5 Tests

ATE_COV.1 Evidence of coverage

Dependencies:

ADV_FSP.2 Security-enforcing functional specification
ATE_FUN.1 Functional testing

Developer action elements:

ATE_COV.1.1D The developer shall provide evidence of the test coverage.

Content and presentation elements:

ATE_COV.1.1C The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.

Evaluator action elements:

ATE_COV.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_FUN.1 Functional testing

Dependencies:

ATE_COV.1 Evidence of coverage

ATE_FUN.1.1D The developer shall test the TSF and document the results.

ATE_FUN.1.2D The developer shall provide test documentation.

Content and presentation elements:

ATE_FUN.1.1C The test documentation shall consist of test plans, expected test results and actual test results.

ATE_FUN.1.2C The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.

ATE_FUN.1.3C The expected test results shall show the anticipated outputs from a successful execution of the tests.

ATE_FUN.1.4C The actual test results shall be consistent with the expected test results.

Evaluator action elements:

ATE_FUN.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2 Independent testing - sample

Dependencies:

ADV_FSP.2 Security-enforcing functional specification

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

ATE_COV.1 Evidence of coverage

ATE_FUN.1 Functional testing

Developer action elements:

ATE_IND.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.2.1C The TOE shall be suitable for testing.

ATE_IND.2.2C The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.

Evaluator action elements:

ATE_IND.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ATE_IND.2.2E The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.

ATE_IND.2.3E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

6.2.6 Vulnerability assessment

AVA_VAN.2 vulnerability analysis

Dependencies:

ADV_ARC.1 Security architecture description

ADV_FSP.2 Security-enforcing functional specification

ADV_TDS.1 Basic design

AGD_OPE.1 Operational user guidance

AGD_PRE.1 Preparative procedures

Developer action elements:

AVA_VAN.2.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.2.1C The TOE shall be suitable for testing.

Evaluator action elements:

AVA_VAN.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

AVA_VAN.2.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3E The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6.3 TOE Security Requirements Rationale

The security requirement must satisfy the security objectives, and as a result, verify that it is appropriate for dealing with security problems.

6.3.1 Security Functional Requirements Rationale

The security requirements rationale shall authenticate the following:

- Each security objective for the TOE is addresses by at least on TOE security functional requirement.
- Each TOE security functional requirement covers at least one security for the TOE.

Table 21 shows mappings between Security Objectives for the TOE and TOE SFRs.

Security Objectives / SFRs	TOE Security Objectives				
	O.Management	O.Audit	O.Iden & Auth	O. Access Control	O. TDI
FCO_NRO.1					X
FCS_COP.1					X
FRN_RNG.1					X
FDP_ACC.1(1)				X	
FDP_ACF.1(1)				X	
FDP_ACC.1(2)				X	
FDP_ACF.1(2)				X	
FIA_AFL.1			X		
FIA_SOS.1			X		
FIA_UAU.7			X		
FIA_UAU.2			X		
FIA_UID.2			X		
FMT_MOF.1	X				
FMT_MSA.1	X				

FMT_MSA.3	X				
FMT_SMF.1	X				
FMT_SMR.1	X				
FPT_TDC.1					X
FAU_ARP.1		X			
FAU_GEN.1		X			
FAU_GEN.2		X			
FAU_SAR.1		X			
FAU_SAR.3		X			
FAU_SAA.1		X			

Table 21 mappings between Security Objectives for the TOE and TOE SFRs

FCS_COP.1 Cryptographic operation
This component satisfies security objectives for the TOE O.Transmitted Data Integrity to ensuring the ability to conduct cryptographic operation according to the specified cryptographic operation algorithms(ECDSA and RSASSA-PSS) and the specified cryptographic key sizes

FRN_RNG.1 Random Number Generator
This component defines random number creation method by TOEs to assure integrity of transmitted data. By specifying random number creation mechanism in FRN_RNG, data integrity between device and TOEs can be assured through trusted random number. Therefore, this component satisfies security objective for the TOE O.Transmitted Data Integrity.

FDP_ACC.1(1) Subset access control
This component defines access control policy for TOEs, TOEa, Authenticator and assures policy definition range. Therefore, this component satisfies security objective for the TOE O. Access control.

FDP_ACF.1(1) Security attribute based access control
This component assures access control policy for TOEs, TOEa, Authenticator execution based on object/subject's security attributes. Therefore, this component satisfies security objective for the TOE O. Access control.

FDP_ACC.1(2) Subset access control
This component defines access control policy of Security Data and assures policy definition range. Therefore, this component satisfies security objective for the TOE O. Access control.

FDP_ACF.1(2) Security attribute based access control
This component assures access control policy of Security Data execution based on object/subject's security attributes. Therefore, this component satisfies security objective for the TOE O. Access control.

FAU_SOS.1 Verification of secrets
This component satisfies security objectives for the TOE O. Identification & Authentication by providing mechanism to verify that secrets meet defined quality metrics.

FAU_AFL.1 Authentication failure handling

This component satisfies the security objective for the TOE O. Identification & Authentication by ensuring the ability to define number of unsuccessful administrator's authentication attempts and take actions when the defined number of unsuccessful authentication attempts has been met

FAU_UAU.2 User authentication before any action
This component satisfies the security objective for the TOE O. Identification & Authentication by ensuring the ability to authentication authorized TOEa user successfully

FAU_UAU.7 Protected authentication feedback
This component satisfies security objectives for the TOE O. Identification & Authentication by ensuring that only specified feedback information is provided to the user during the authentication.

FAU_UID.2 User identification before any action
This component satisfies the security objective for the TOE O. Identification & Authentication by ensuring the ability to identify TOEa user successfully.

FMT_MOF.1 Management of security functions behaviour
This component satisfies the security objective for the TOE O .Management by ensuring the ability to manage security features by authorized administrators.

FMT_MSA.1 Management of security attributes
This component satisfies the security objective for the TOE O. Management by ensuring the ability to manage security attributes used for the FDP_ACC.1(1), FDP_ACC.1(2) policy by authorized administrators.

FMT_MSA.3 Static attribute initialisation
This component satisfies the security objective for the TOE O. Management by providing authorized administrator roles to specify alternative initial values to override the default values of security attributes used for the FDP_ACC.1(1), FDP_ACC.1(2) policy.

FMT_SMF.1 Specification of management functions
This component satisfies the security objective for the TOE O. Management by ensuring the ability to specify management functions related to security attributes, TSF data, security functions.

FMT_SMR.1 Security roles
This component satisfies the security objective for the TOE O. Management by ensuring that users are associated with the authorized administrator role.

FPT_TDC.1 Inter-TSF basic TSF data consistency
This component assures consistency of TSF data transmitted between TSF. Signed data transmitted from device to TOEs is formed as required by Authenticator before transmitted, so data remains consistent and TOEs read this data with consistency. Therefore, this component satisfies security objective for the TOE O. Transmitted data integrity.

FAU_ARP.1 Security alarms
This component satisfies the security objective for the TOE O.Audit by ensuring the ability to take the response in case of detected events indicative of security violation.

FAU_GEN1. Audit data generation

This component satisfies the security objective for the TOE O.Audit by ensuring the ability to define auditable events and generate audit records.

FAU_GEN.2 User identity association
This component satisfies the security objective for the TOE O.Audit by ensuring the ability to associate each auditable event with the identity of the user that caused the audit event.

FAU_SAR.1 Audit review
This component satisfies the security objective for the TOE O. Audit by ensuring the ability to review audit records by authorized administrators.

FAU_SAR.3 Selectable audit review
This component satisfies the security objective for the TOE O. Audit by ensuring the ability to select the audit data to be reviewed based on criteria.

FAU_SAA.1 Potential violation analysis
This component satisfies the security objective for the TOE O. Audit by ensuring the ability to detect the violation event..

FCO_NRO.1 Selective proof of origin
This component satisfies the security objective for the TOE O. Transmitted Data Integrity by ensuring the ability to verify the digital signature to ensure the non-repudiation.

6.3.2 TOE Security assurance requirements

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

EAL2 requires evidence relating to the design information and test result, 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 behavior.

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 user of configuration management system and evidence of secure delivery procedures.

6.3.3 Dependency of TOE Security Functional Requirements

The following table shows the dependencies of the security functional requirements.

No.	SFRs	Dependencies	Reference
0	FRN_RNG.1	none	none
1	FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FMT_CKM.4	- -

2	FDP_ACC.1(1)	FDP_ACF.1(1)	3
3	FDP_ACF.1(1)	FDP_ACC.1(1), FMT_MSA.3	2 12
4	FDP_ACC.1(2)	FDP_ACF.1(2)	5
5	FDP_ACF.1(2)	FDP_ACC.1(2), FMT_MSA.3	4 14
6	FPT_TDC.1	none	none
7	FIA_AFL.1	FIA_UAU.2	10
8	FIA_SOS.1	none	none
9	FIA_UAU.7	FIA_UAU.2	10
10	FIA_UAU.2	FIA_UID.2	11
11	FIA_UID.2	none	none
12	FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	15 16
13	FMT_MSA.1	FDP_ACC.1(1)(2) FMT_SMF.1 FMT_SMR.1	2, 4 15 16
14	FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	13 16
15	FMT_SMF.1	none	none
16	FMT_SMR.1	FIA_UID.2	-
17	FAU_ARP.1	FAU_SAA.1	22
18	FAU_GEN.1	FPT_STM.1(provided by SP)	-
19	FAU_GEN.2	FAU_GEN.1 FIA_UID.2	18 10
20	FAU_SAR.1	FAU_GEN.1	18
21	FAU_SAR.3	FAU_SAR.1	20
22	FAU_SAA.1	FAU_GEN.1	18
23	FCO_NRO.1	FIA_UID.1	-

Table 22 Dependencies of SFRs

Theoretical Basis for subordinated components

① FCS_CKM.1(user Private Key, user Public Key creation), which is in a lower hierarchy of FCS_COP.1, is not included in TOE, because Authenticator, which is TOE operation environment, manages FCS_CKM.1 in case of Registration. Attestation Private Key and Attestation Public Key are provided by Authenticator's manufacturer and stored in secure storage of the device, thus FCS_CKM.1 is not part of TOE.
FCS_CKM.4 is not included in TOE, because Attestation Private Key and user Private Key destruction is part of Authenticator's role. Attestation Public Key and user Public Key is managed by TOEs, but it modifies the Flag value of the keys to '1' instead of physically destroying them to check repudiation.

② FPT_STM.1, which is in a lower hierarchy of FAU_GEN.1, is not included in TOE, because it should be provided in SP, the TOE operation environment.

③ FIA_UID.1, which is in a lower hierarchy of FCO_NRO.1 is not included in TOE, because TOE operation environment should be provided in FIDO Client.

7 TOE Summary Specification

This chapter describes how TOE features meet the security requirements by introducing subsystems and defines TOE guarantee-methods to comply with the security requirements

TOE Security Features

This sub-chapter illustrates the security features of TOE to comply with the defined 'TOE security requirements' by explaining the mechanism of the subsystems. TOE consists of 13 subsystems, and jointed action of the subsystems meets the security requirements.

7.1 TOEs Security Features

TOEs assures the data integrity by verifying the digital signature with private key generated and transmitted from Authenticator using public key. And TOEs can prevent the replay-attack by generating a random number (Challenge) and verifying the number.

Based on access control policy, when installing TOEs, only authorized administrators can have access to data such as Authenticator's metadata, SP information and so on. Also, TOEs restricts unauthorized SP Server or TOEa using the unique key(API Key). And TOEs can detect the duplication of Authenticator by using Signature Counter.

7.1.1 UAF(UAFS)

UAF, a sub-system called upon SP Server requests, executes subsequent process based on UAF Operation (Registration, Authentication, Transaction Confirmation, and Deregistration)

Related SFR

FPT_TDC.1, FAU_GEN.1, FAU_GEN.2

7.1.2 License Engine(LE)

License Engine verifies TOE's license so that only authorized SP Server can be access to the TOEs.

Related SFR

none

7.1.3 Challenge Engine (CES)

Challenge Engine generates the random bytes in the server challenge field contained in UAF Request Message and transmits it to FIDO Client. The server challenge is signed by Authenticator and contained in UAF Response Message. The UAF Response Message is transmitted to TOEs, and CE assures the integrity of UAF Response Message by verifying the server challenge.

Related SFR

FCO_NRO.1, FRN_RNG.1

7.1.4 Crypto Engine(CE)

Crypto Engine is used when verifying the digital signature generated by Authenticator with public key in registration, authentication, and transaction confirmation case. It is a sub-system in charge of cryptographic operation. It is used for assuring the integrity of the digital signature transmitted from the device. ECDSA/RSA and SHA-256 Hash algorithm are used for the digital signature algorithm.

Related SFR
FCO_NRO.1, FCS_COP.1

7.1.5 Policy Engine(PE)

Policy Engine constructs appropriate authentication policy of SP contained in UAF Request Message and transmitted to FIDO Client. When TOEs receives the UAF Response Message, PE can verify the policy if it does match the initial policy.

Related SFR
none

7.1.6 Trusted Facet Engine(TFE)

Trusted Facet Engine manages FacetList. When FIDO Client requests a FacetList, TFE sends it to FIDO Client. And when UAF Response message is received, TFE verifies FacetID to detect if it is accessed through authorized App or not.

Related SFR
none

7.1.7 Attestation Engine(AE)

Attestation Engine assures the integrity of signed data generated by Authenticator.

Related SFR
FCO_NRO.1, FDP_ACC.1(1), FDP_ACF.1(1)

7.1.8 RP Manager(RM)

RP Manager is called when authorized administrators (delivery manager/SP operation administrator/SP operator) of TOEa register or modify SP information (RP ID, API Key, App ID, FacetList, Policy, Etc.) through UI. RM checks if SP Server or TOEa is authorized by verifying API Key.

Related SFR
FDP_ACC.1(1), FDP_ACF.1(1), FMT_MOF.1, FMT_MSA.3, FMT_SMF.1,

7.1.9 Metadata Manager(MM)

Metadata Manager is called when authorized administrators of TOEa register, modify, or Authenticator Metadata (AAID (Authenticator Attestation ID), Authenticator Version, Attestation Root Certificates, Etc) through UI or when verifying the signed data transmitted from the device.

Related SFR
FMT_MOF.1, FMT_MSA.3, FMT_SMF.1

7.2 TOEa Security Features

TOEa, as an audit of TOE, generates or searches audit data regarding security related issues. Only authorized administrators can register/modify/remove users, audit log in history, and control access to TOE assets by managing writing/changing rights for Authenticator Metadata and SP information.

7.2.1 User Manager(UM)

User Manager manages menu and user role, manages data, such as TOEa user registration, modify, or remove, and provides log in/log out features

Related SFR
FIA_AFL.1, FIA_SOS.1, FIA_UAU.2, FIA_UID.2, FIA_UAU.7, FDP_ACC.1(2), FDP_ACF.1(2), FMT_MOF.1, FMT_SMF.1, SMT_SMR.1

7.2.2 Log Manager(LM)

Log Manager creates audit history of TOE. Log Manager collects user log in history and admin activity history from TOEa

Related SFR
FAU_ARP.1, FAU_GEN.1, FAU_GEN.2, FAU_SAA.1, FAU_SAR.1

7.2.3 License Manager(LSM)

License Manager registers/modifies/removes TOEs licenses.

Related SFR
none

7.2.4 Statistics Manager(SM)

Statistics Manager collects information from Log Manager, and reforms it as statistics

Related SFR
none

7.2.5 UI(UI)

UI delivers input data from users to relevant sub-system.

Related SFR
FAU_SAR.3

Glossary

Terminology	Description
FIDO(Fast IDentity Online)	Online user authentication method using device based authentication mechanism, such as fingerprint recognition, iris recognition, or PIN verification.
FIDO Alliance	A non-profit organization formed in 2012 to address the global standard protocol and technical specification to use user's biometric information with members of Google, MS, Samsung Electronics, Master Card, etc.
UAF(Universal Authentication Framework)	International standard of authentication method defined by FIDO 1.0
FIDO UAF Protocol	Communication protocol for FIDO UAF Message between user device and Service Provider
FIDO Server	Server entity on FIDO UAF protocol side. Interacts with SP Web Server to exchange UAF protocol message with FIDO Client Inspects trusted authenticator through metadata verification, and evaluates credibility of user authentication and payment transaction information.
FIDO Client	Software entity which processes UAF protocol message on FIDO user device. Communicates with Authenticator through API and communicates with FIDO Server by interacting with users through device interface.
Admin Portal	Web based Admin page that provides features, such as FIDO Server configuration change, license management, and service history and statistics management.
Service Provider(Relying Party)	Entity that uses FIDO protocol for user authentication
SP Server	SP Application that runs on server side and answers to HTTP requests.
SP App	SP Application built on open web platform that runs on user side.
ASM (Authenticator Specific Module)	Software that provides API so that FIDO Client can communicate with Authenticator of device.
Authenticator	Creates Key for FIDO UAF authentication in secured area inside the user device.
Discovery	Activity of discovering the Authenticator that works with FIDO among authenticators for device.
Registration	Activity of registering the device online by storing public key on FIDO Server after creating private and public key in Secure H/W of device.
Authentication	Activity of authenticating a user on FIDO Server using public and private key after entering a PIN or putting in biometric information in the device.

Transaction Confirmation	Transaction Confirmation happens during Authentication when contents contain confirmation; for example, payment transaction.
Deregistration	Activity of erasing a public key from FIDO Server and private key from Authenticator
PKI(Public Key Infrastructure)	Authentication system that uses private key and public key. Private key is used to sign the data. Public key is used to verify the digital signature.
Private Key	Key that only key owner can recognize.
Public Key	Key that other entity can use
Attestation Private key	This is pre-stored on a local device with Attestation Certificate. Authenticator signs the registration data transmitted to TOEs with Attestation Private key during registration.
Attestation Certificate	A public key certificate related to an Attestation Key.
User's Private key	This is created by Authenticator during Authentication. User's Private key is used to sign the authentication data.
User's Public Key	This is created by Authenticator during Authentication. User's Public key is used to verify the digital signature generated by Authenticator.
Time Stamp	Parameter that indicates specific time frame
Hash	Algorithm that maps random length of data into certain length of data.
TLS(Transport Layer Security)	Encryption protocol for TCP/IP network communication which is used for protecting data transmitted between FIDO Server and FIDO Client.
Biometrics Information	Information based on person's own and unique body structure and components.
PIN(personal identification number)	Personal Identification Number which is used to verify identification.
AAID(Authenticator Attestation ID)	ID that each Authenticator has to identify if UAF can authenticate. AAID is composed of Authenticator manufacturer information and model information.
API Key	Value that is used for checking if it is trusted access when FIDO Server API is called from Admin Portal or SP. API Key is created when registering SP or Admin Portal on FIDO Server.
AppID	URL indicating TrustedFacet List (FacetID) by RP.
FacetID	OS/Platform Identifier for cases where one SP App is on several different OS/Platforms.
FacetList	List data architecture for FacetID, and AppID is used to have this architecture
KeyID	ID to identify UAuth.Key that is created by Authenticator.
ServerChallenge	Random value produced by FIDO Server, which is used for verifying response message that FIDO Server received.

FinalChallenge	Data created in FIDO client using value of AppID, challenge, facetID, channelBinding
License	Certificate that product manufacturer produces to protect the product information. Through license verification process, only authorized SP Server works for FIDO
Metadata	Data of authorized Authenticator
Policy	JSON data architecture used for transmitting data, such as Authenticator specification or information, to FIDO Client when operating FIDO
SecurityWarning	Security Warning is provided in Admin Portal for administrators to examine the cause when there is any FIDO activity failure due to any security related reason.
BlackList	Blacklist extracts problematic users from Security Warning and manages them on a blacklist to avoid further problems
Delivery Manager	Deploys and installs TOE based on the installation manual.
Operation Administrator	Group of users who can manage user data, license, SP, Metadata, and check service history and statistics of FIDO through Admin Portal.
Operator	Group of users who can check service history and statistics of FIDO through Admin Portal.

Reference

[1] FIDO Technical Glossary
https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-glossary-v1.0-ps-20141208.html

[2] FIDO UAF Protocol Specification v1.0
https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-20141208.html

[3] FIDO UAF Architectural Overview
https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-overview-v1.0-ps-20141208.html

[4] FIDO UAF Registry of Predefined Values
https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-reg-v1.0-ps-20141208.html

[5]FIDO UAF Authenticator Metadata Statements v1.0
https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-authnr-metadata-v1.0-ps-20141208.html

[6] FIDO AppID and Facet Specification v1.0
https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-appid-and-facets-v1.0-ps-20141208.html

[7] FIDO Alliance Site
https://fidoalliance.org/specifications/overview/

END OF DOCUMENT