SDS FIDO V1.1 Security Target Lite

Sep 2, 2015

Solution Group (SC_MA)
Smart Convergence Business Unit
# Contents

Contents........................................................................................................................................... 1

List of Figures ................................................................................................................................... 4

List of Tables ...................................................................................................................................... 5

1  Security Target Instruction.............................................................................................................. 6

  1.1  Security Target Reference........................................................................................................ 6

  1.2  TOE Reference......................................................................................................................... 6

  1.3  TOE Overview........................................................................................................................ 7

     1.3.1  Usage and Major Security Features of the TOE................................................................. 7

  1.4  TOE Description....................................................................................................................... 9

     1.4.1  Required non-TOE Hardware/Software.......................................................................... 9

     1.4.2  Physical scope of TOE.................................................................................................... 11

     1.4.3  Logical scope of TOE...................................................................................................... 12

  1.5  Document Organization........................................................................................................... 13

2  Conformance Claim......................................................................................................................... 15

  2.1  Common Criteria Conformance Claim.................................................................................... 15

  2.2  Protection Profile Claim.......................................................................................................... 15

  2.3  Package Claim........................................................................................................................ 15

  2.4  Preparation Rules ................................................................................................................... 15

3  Security Problem Definition........................................................................................................... 16

  3.1  Threats..................................................................................................................................... 16

     3.1.1  Threats from the device .................................................................................................. 16

     3.1.2  Threats to the TOEs....................................................................................................... 16

     3.1.3  Threats to the TOEa ..................................................................................................... 16

  3.2  Organizational Security Policies............................................................................................ 16
6.3 TOE Security Requirements Rationale ................................................................. 46

6.3.1 Security Functional Requirements Rationale .................................................... 46

6.3.2 TOE Security assurance requirements ............................................................... 49

6.3.3 Dependency of TOE Security Functional Requirements .................................... 49

7 TOE Summary Specification ..................................................................................... 51

7.1 TOEs Security Features ......................................................................................... 51

7.1.1 UAF(UAFS) ........................................................................................................ 51

7.1.2 License Engine(LE) ........................................................................................... 51

7.1.3 Challenge Engine (CES) ................................................................................... 51

7.1.4 Crypto Engine(CE) ............................................................................................ 51

7.1.5 Policy Engine(PE) ............................................................................................ 52

7.1.6 Trusted Facet Engine(TFE) ................................................................................ 52

7.1.7 Attestation Engine(AE) .................................................................................... 52

7.1.8 RP Manager(RM) ............................................................................................. 52

7.1.9 Metadata Manager(MM) ................................................................................... 52

7.2 TOEa Security Features ....................................................................................... 52

7.2.1 User Manager(UM) .......................................................................................... 52

7.2.2 Log Manager(LM) ............................................................................................ 53

7.2.3 License Manager(LSM) .................................................................................... 53

7.2.4 Statistics Manager(SM) ................................................................................... 53

7.2.5 UI(UI) ................................................................................................................ 53

Glossary ....................................................................................................................... 54

Reference ..................................................................................................................... 57
List of Figures

Picture 1 TOE Operation Environment ................................................................. 8
Picture 2 Physical Architecture of IDC environment .............................................. 11
Picture 3 Physical Architecture of Cloud environment ......................................... 11
Picture 4 Random number class component ......................................................... 25
Picture 5 Random number creation components and hierarchy ............................. 25
List of Tables

Table 1 Non-TOE Hardware/Software required in TOE........................................................... 10
Table 2 Menu Access by User................................................................................................... 17
Table 3 The mapping between Security Environment and Security Objectives..................... 21
Table 4 Security Problem Definition and Security Objectives Action / Theoretical Basis........... 24
Table 5 Random number class composition.......................................................................... 25
Table 6 TOE Security Functional Requirements.................................................................... 27
Table 7 Digital Signature Algorithm [4]................................................................................ 28
Table 8 Operation for Subject & Object.................................................................................. 29
Table 9 Access Rule by Detailed Security Attributes.............................................................. 29
Table 10 Functions by Information.......................................................................................... 30
Table 11 Operation by Subject & Object................................................................................. 30
Table 12 Access Rule by detailed security attributes............................................................. 31
Table 13 Security Attribute of secrets.................................................................................... 31
Table 14 Function by Authorized Roles.................................................................................. 32
Table 15 Security Attributes-Action by Authorized Role......................................................... 33
Table 16 Audit Event................................................................................................................. 34
Table 17 list of Potential violation............................................................................................ 35
Table 18 Key Registration Data[5]........................................................................................ 37
Table 19 Signed Data[5]......................................................................................................... 37
Table 20 Security Assurance Requirements............................................................................ 38
Table 21 mappings between Security Objectives for the TOE and TOE SFRs....................... 47
Table 22 Dependencies of SFRs.............................................................................................. 50
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.


\(^2\) 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.

**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.
<table>
<thead>
<tr>
<th>Type</th>
<th>Category</th>
<th>OS</th>
<th>Minimum H/W Requirement</th>
<th>S/W</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>CPU</td>
<td>MEM</td>
</tr>
<tr>
<td>Admin Portal</td>
<td>Red Hat Enterprise Linux Server release 5.8</td>
<td>Intel Core i7 2.2GHz, 4Core</td>
<td>4GB RAM</td>
<td>10/100/1000 ethernet*1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB Server</td>
<td>Red Hat Enterprise Linux Server release 5.8</td>
<td>Intel Core i7 2.0GHz, 4Core</td>
<td>4GB RAM</td>
<td>10/100/1000 ethernet*1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Portal Console</td>
<td>Windows 7 Enterprise K (32bit/64bit)</td>
<td>PENTIUM 2.0 Ghz</td>
<td>1GB RAM</td>
<td>10/100/1000 ethernet*1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIDO Server</td>
<td>Ubuntu 12.04 server Enterprise</td>
<td>Intel Xeon CPU X5670 Hexa 2.9GHz, 2Core</td>
<td>8GB RAM</td>
<td>Emulex 10G 2Port NIC * 2, Broadcom 1G * 4Port(On-B’d)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB Server</td>
<td>Red Hat Enterprise Linux Server release 6.5</td>
<td>Intel Xeon CPU X5670 Hexa 2.9GHz, 2Core</td>
<td>16GB RAM</td>
<td>Emulex 10G 2Port NIC * 2, Broadcom 1G * 4Port(On-B’d)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SP Server</td>
<td>Ubuntu 12.04 server Enterprise</td>
<td>Intel Xeon CPU X5670 Hexa 2.9GHz, 2Core</td>
<td>4GB RAM</td>
<td>Emulex 10G 2Port NIC * 2, Broadcom 1G * 4Port(On-B’d)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Admin Portal Console</td>
<td>Windows 7 Enterprise K (32bit/64bit)</td>
<td>PENTIUM 2.0 Ghz</td>
<td>1GB RAM</td>
<td>10/100/1000 ethernet*1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Galaxy S6 (SM-G920) / Galaxy S6 edge (SM-G925) | FIDO Client | Android 5.0 | 2.1GHz / 1.5GHz Octa-Core | 3GB | 32GB / 64GB(ROM) |
|                                             | ASM | N/A | N/A | N/A | N/A |
|                                             | Authenticator | N/A | N/A | N/A | 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.

**RP³ 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

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.

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

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.

<table>
<thead>
<tr>
<th>Security Problem Definition</th>
<th>Security Objectives</th>
<th>Security Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>T. CAA</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>T. Damage to Stored Data</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>T. Replay Attack</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>T. Transmitted Data Forgery</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>T. Authenticator Duplication</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>T. ASM &amp; FIDO Client Duplication</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>T. Illegal Access</td>
<td>X</td>
<td>×</td>
</tr>
<tr>
<td>P. Audit</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>P. SP Development Guideline</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>P. Installation and Delivery</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>P. User Access Management</td>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>A. Secure Storge</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>A. Robust Cryptography Alg</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>A. Protocol Compliance</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>A. Secure CC</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>A. Reliable Device Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A. Trusted IT Environment</td>
<td>×</td>
<td></td>
</tr>
<tr>
<td>A. Timestamp</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>A. DBMS</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Table 3 The mapping between Security Environment and Security Objectives

※ CAA : Consecutive Attempt Authentication  ※ TDC : Transmitted Data Confidentiality
※ TDI : Transmitted Data Integrity  ※ TIE : Trusted IT Environment
※ SKM : Secure Key Management  ※ RDE : Reliable Device Environment
<table>
<thead>
<tr>
<th>Security Problem</th>
<th>Security Objective to be Mapped</th>
<th>Theoretical Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td>T. Consecutive Attempt to Authentication</td>
<td>O. Identification and Authentication</td>
<td>O. Identification and Authentication: Since the TOEs provides the access to delivery manager, operation administrator and operator before starting the security management operation and TOEs can’t be accessed after five consecutive authentication failures, it takes action against T. Consecutive Attempt To Authentication.</td>
</tr>
</tbody>
</table>
| 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 O. 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.  
O. 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. |
<table>
<thead>
<tr>
<th>T. ASM and FIDO Client Duplication</th>
<th>OE. Reliable Device Environment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OE. Reliable Device Environment</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>T. Illegal Access</th>
<th>O. Access Control (TOEs)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>O. Access Control (TOEs)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>O. Access Control (TOEs)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P. Audit</th>
<th>O. Audit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>O. Audit:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P. SP Development Guideline</th>
<th>OE. Protocol Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OE. Protocol Compliance</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>P. Delivery</th>
<th>O. Management &amp; OE. Management</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>O. Management &amp; OE. Management:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Security Problem Definition / Security Objectives</td>
<td>Action</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td><strong>P. User Access Management</strong></td>
<td>O. Access Control</td>
</tr>
<tr>
<td></td>
<td>O. Management</td>
</tr>
<tr>
<td><strong>A. Secured Storage</strong></td>
<td>OE. Secured Key Management</td>
</tr>
<tr>
<td><strong>A. Robust Cryptography Algorithm</strong></td>
<td>OE. Transmitted Data Integrity</td>
</tr>
<tr>
<td><strong>A. Protocol Compliance</strong></td>
<td>OE. Protocol Compliance</td>
</tr>
<tr>
<td><strong>A. Secure Communication Channel</strong></td>
<td>OE. Transmitted Data Confidentiality</td>
</tr>
<tr>
<td><strong>A. Reliable Device Environment</strong></td>
<td>OE. Reliable Device Environment</td>
</tr>
<tr>
<td><strong>A. Trusted IT Environment</strong></td>
<td>OE. Trusted IT Environment</td>
</tr>
<tr>
<td><strong>A. Timestamp</strong></td>
<td>OE. Timestamp</td>
</tr>
<tr>
<td><strong>A. DBMS</strong></td>
<td>OE.DBMS</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Security Functional Class</th>
<th>Security Functional Component</th>
</tr>
</thead>
<tbody>
<tr>
<td>Random Number</td>
<td>FRN_RNG.1(Extended)</td>
</tr>
<tr>
<td></td>
<td>Random Number Generator</td>
</tr>
</tbody>
</table>

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.

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

<table>
<thead>
<tr>
<th>FRN_RNG Random Number Generator</th>
<th>1</th>
</tr>
</thead>
</table>

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]
## 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.

<table>
<thead>
<tr>
<th>Security Functional Class</th>
<th>Level</th>
<th>Functional Family</th>
<th>Security objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCS: Cryptographic Support</td>
<td>FCS_COP.1</td>
<td>FCS_COP, Cryptographic operation</td>
<td>O. Transmitted Data Integrity</td>
</tr>
<tr>
<td>FRN: Random Number</td>
<td>FRN_RNG.1</td>
<td>FRN_RNG, Random Number Generation</td>
<td>O. Transmitted Data Integrity</td>
</tr>
<tr>
<td>FDP: User Data Protection</td>
<td>FDP_ACC.1(1)</td>
<td>FDP_ACC, Access control policy</td>
<td>O. Access Control</td>
</tr>
<tr>
<td></td>
<td>FDP_ACF.1(1)</td>
<td>FDP_ACF, Access control functions</td>
<td>O. Access Control</td>
</tr>
<tr>
<td></td>
<td>FDP_ACC.1(2)</td>
<td>FDP_ACC, Access control policy</td>
<td>O. Access Control</td>
</tr>
<tr>
<td></td>
<td>FDP_ACF.1(2)</td>
<td>FDP_ACF, Access control functions</td>
<td>O. Access Control</td>
</tr>
<tr>
<td>FIA, Identification &amp; authentication</td>
<td>FIA_AFL.1</td>
<td>FIA_AFL, Authentication failures</td>
<td>O. Identification &amp; authentication</td>
</tr>
<tr>
<td></td>
<td>FIA_SOS.1</td>
<td>FIA_SOS, Specification of secrets</td>
<td>O. Identification &amp; authentication</td>
</tr>
<tr>
<td></td>
<td>FIA_UAU.7</td>
<td>FIA_UAU, User authentication</td>
<td>O. Identification &amp; authentication</td>
</tr>
<tr>
<td></td>
<td>FIA_UAU.2</td>
<td>FIA_UAU, User authentication</td>
<td>O. Identification &amp; authentication</td>
</tr>
<tr>
<td></td>
<td>FIA_UID.2</td>
<td>FIA_UID, User identification</td>
<td>O. Identification &amp; authentication</td>
</tr>
<tr>
<td>FMT, Security management</td>
<td>FMT_MOF.1</td>
<td>FMT_MOF, Management of function in TSF</td>
<td>O. Management</td>
</tr>
<tr>
<td></td>
<td>FMT_MSA.1</td>
<td>FMT_MSA, Management of security attributes</td>
<td>O. Management</td>
</tr>
<tr>
<td></td>
<td>FMT_MSA.3</td>
<td>FMT_MSA, Management of security attributes</td>
<td>O. Management</td>
</tr>
<tr>
<td></td>
<td>FMT_SMF.1</td>
<td>FMT_SMF, Specification of Management Functions</td>
<td>O. Management</td>
</tr>
<tr>
<td></td>
<td>FMT_SMR.1</td>
<td>FMT_SMR, Security management roles</td>
<td>O. Management</td>
</tr>
<tr>
<td>FPT, Protection of the TSF</td>
<td>FPT_TDC.1</td>
<td>FPT_TDC, Inter-TSF TSF data consistency</td>
<td>O. Transmitted Data Integrity</td>
</tr>
<tr>
<td>FAU, Security Audit</td>
<td>FAU_ARP.1</td>
<td>FAU_ARP, Security audit automatic response</td>
<td>O. Audit</td>
</tr>
<tr>
<td></td>
<td>FAU_GEN.1</td>
<td>FAU_GEN, Security audit data generation</td>
<td>O. Audit</td>
</tr>
<tr>
<td></td>
<td>FAU_GEN.2</td>
<td>FAU_GEN, Security audit data generation</td>
<td>O. Audit</td>
</tr>
<tr>
<td>FAU_SAR.1</td>
<td>FAU_SAR, Security audit review</td>
<td>0. Audit</td>
<td></td>
</tr>
<tr>
<td>FAU_SAR.3</td>
<td>FAU_SAR, Security audit review</td>
<td>O. Audit</td>
<td></td>
</tr>
<tr>
<td>FAU_SAA.1</td>
<td>FAU_SAA, Security audit analysis</td>
<td>O. Audit</td>
<td></td>
</tr>
<tr>
<td>FCO, Communication</td>
<td>FCO_NRO.1</td>
<td>FCO_NRO, Non-repudiation of origin</td>
<td>O. Transmitted Data Integrity</td>
</tr>
</tbody>
</table>

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]

<table>
<thead>
<tr>
<th>List of standards</th>
<th>Signature Algorithm</th>
<th>Cryptographic key sizes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECDSA Signature ANSI X9.62-2005</td>
<td>SECP25 6R1_EC DSA_S HA256_RAW</td>
<td>256bit</td>
<td>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)]</td>
</tr>
<tr>
<td></td>
<td>SECP25 6R1_EC DSA_S HA256_DER</td>
<td>256bit</td>
<td>DER [ITU-X690-2008] encoded ECDSA signature [RFC5480] on the NIST secp256r1 curve. I.e. a DER encoded SEQUENCE { r INTEGER, s INTEGER }</td>
</tr>
<tr>
<td></td>
<td>SECP25 6K1_EC DSA_S HA256_RAW</td>
<td>256bit</td>
<td>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)]</td>
</tr>
<tr>
<td></td>
<td>SECP25 6K1_EC DSA_S HA256_DER</td>
<td>256bit</td>
<td>DER [ITU-X690-2008] encoded ECDSA signature [RFC5480] on the secp256k1 curve. I.e. a DER encoded SEQUENCE { r INTEGER, s INTEGER }</td>
</tr>
</tbody>
</table>
RSASSA-PSS signature [RFC3447], [RFC4055], [RFC4056]

<table>
<thead>
<tr>
<th>Signature Type</th>
<th>Algorithm</th>
<th>Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSASSA-PSS [RFC3447]</td>
<td>Mask Generation Algorithm MGF1 with SHA256</td>
<td>256-bit</td>
</tr>
<tr>
<td>RSASSA-PSS [RFC3447]</td>
<td>Salt Length of 32 bytes, i.e. the length of a SHA256 hash value.</td>
<td></td>
</tr>
<tr>
<td>RSASSA-PSS [RFC3447]</td>
<td>Trailer Field value of 1, which represents the trailer field with hexadecimal value 0xBC.</td>
<td></td>
</tr>
</tbody>
</table>

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].

<table>
<thead>
<tr>
<th>SFP</th>
<th>Subject</th>
<th>Subjects Security Attribute</th>
<th>Object</th>
<th>Objects Security Attribute</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>SP Server</td>
<td>IT entity using SP</td>
<td>API Key</td>
<td>TOEs</td>
<td>API Key</td>
<td>TOEs Access</td>
</tr>
</tbody>
</table>
### Table 8 Operation for Subject & Object

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Server</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticator Access Control</td>
<td>IT entity using Authenticator</td>
<td>Signature Counter</td>
</tr>
<tr>
<td>TOEa Access Control</td>
<td>IT entity using TOEa</td>
<td>API Key</td>
</tr>
</tbody>
</table>

### 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].

<table>
<thead>
<tr>
<th>Detailed Security Attribute</th>
<th>Access Control Rule</th>
<th>Access Authorization Rule</th>
<th>Access Denial Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Key</td>
<td>To verify that the API Key of SP server is identical to the API Key stored on TOEs</td>
<td>SP Server is allowed to access TOEs when the API Key matches</td>
<td>SP Server is denied to access TOEs when API Key does not match</td>
</tr>
<tr>
<td>Signature Counter</td>
<td>To compare Authenticator’s Signature Counter to TOEs’ Signature Counter</td>
<td>TOEs is allowed to access if Authenticator’s Signature counter is greater than TOEs’ Signature counter</td>
<td>TOEs is denied to access if Authenticator’s Signature counter is the same or smaller than TOEs’ Signature counter</td>
</tr>
<tr>
<td>API Key</td>
<td>To verify that the API Key of Admin Portal server is identical to the API Key saved on TOEs</td>
<td>TOEa is allowed to access TOEs when the API Key does match</td>
<td>TOEa is denied to access TOEs when API Key does not match</td>
</tr>
</tbody>
</table>
### Table 10 Functions by Information

<table>
<thead>
<tr>
<th>Master Data Management</th>
<th>Service Provider Information</th>
<th>Add, modify, inquire</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Management</td>
<td>User Information</td>
<td>Add, modify, delete, inquire</td>
</tr>
<tr>
<td></td>
<td>Admin History, Login History</td>
<td>Inquire</td>
</tr>
</tbody>
</table>

### Table 11 Operation by Subject & Object

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Users</td>
<td>Operator is not allow to access to the Master Data Management, System Management menu because the operator has ‘Users’ security attributes</td>
<td>N/A</td>
<td>If detail security attribute is ‘Users’, access to Master Data Management and System Management menu is denied</td>
</tr>
<tr>
<td>Administrators</td>
<td>Delivery Manager and Operation Administrator is allowed to add, modify and delete Master Data Management, System Management menu</td>
<td>When detailed security attribute is ‘Administrators’, Master Data Management and System Management menu is accessible</td>
<td>N/A</td>
</tr>
</tbody>
</table>
because they have 'Administrators’ security attributes

<table>
<thead>
<tr>
<th>Security Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>Min8 ~ Max 20 characters in length</td>
</tr>
</tbody>
</table>
| 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]

<table>
<thead>
<tr>
<th>List of functions</th>
<th>Authorized Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add, Modify, Inquire Authenticator Meta</td>
<td>Delivery Manager, Operation Administrator</td>
</tr>
<tr>
<td>Add, Modify, Inquire Service Provider Info</td>
<td></td>
</tr>
<tr>
<td>Add, Modify, Inquire User Info</td>
<td></td>
</tr>
<tr>
<td>Inquire Admin History</td>
<td></td>
</tr>
<tr>
<td>Inquire Login History</td>
<td></td>
</tr>
<tr>
<td>Activation, Deactivation of User Account</td>
<td></td>
</tr>
<tr>
<td>Delete, Inquire Security Warning</td>
<td>Operation Administrator, Operator</td>
</tr>
<tr>
<td>Add, Delete, Inquire BlackList</td>
<td></td>
</tr>
<tr>
<td>Add API Key of TOEa</td>
<td>Delivery Manager</td>
</tr>
</tbody>
</table>

**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
### Table 15 Security Attributes-Action by Authorized Role

<table>
<thead>
<tr>
<th>Security Attributes</th>
<th>Detailed Security Attribute</th>
<th>Action</th>
<th>Authorized Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>GroupName</td>
<td>Users</td>
<td>select</td>
<td>Delivery Manager, SP Operation Administrator</td>
</tr>
<tr>
<td></td>
<td>Administrators</td>
<td></td>
<td></td>
</tr>
<tr>
<td>API Key(SP Server의)</td>
<td>N/A</td>
<td>Initialization, Query, Register, Modify</td>
<td>Delivery Manager, SP Operation Administrator</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>SFRs</th>
<th>Audit data</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIA_AFL.1</td>
<td>Identification/Authentication failure history of administrator</td>
</tr>
<tr>
<td>FIA_UAU.2</td>
<td>Identification/Authentication success / failure history of administrator</td>
</tr>
<tr>
<td>FIA_UID.2</td>
<td>Identification/Authentication success / failure history of administrator</td>
</tr>
<tr>
<td>FMT_MOF.1</td>
<td>TSF data management history by administrator</td>
</tr>
<tr>
<td>FCO_NRO.1</td>
<td>Digital Signature Verification failure history</td>
</tr>
<tr>
<td>FAU_ARP.1</td>
<td>Security Warning history</td>
</tr>
</tbody>
</table>

**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]

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

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_SAR.1.2 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]

<table>
<thead>
<tr>
<th><strong>Key Registration Data</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>AAID</td>
<td>Authenticator Attestation ID</td>
</tr>
<tr>
<td>AuthenticatorVersion</td>
<td>Vendor assigned authenticator version</td>
</tr>
<tr>
<td>AuthenticationMode</td>
<td>Registration or Authentication</td>
</tr>
<tr>
<td>SignatureAlgAndEncoding</td>
<td>Signature Algorithm and Encoding of attestation signature</td>
</tr>
<tr>
<td>PublicKeyAlgAndEncoding</td>
<td>Public Key algorithm and encoding of the newly generated Uauth.pub key</td>
</tr>
<tr>
<td>FinalChallenge</td>
<td>Final Challenge</td>
</tr>
<tr>
<td>KeyID</td>
<td>KeyID generated by Authenticator</td>
</tr>
<tr>
<td>SignCounter</td>
<td>Indicates how many times this authenticator has performed signatures in the past.</td>
</tr>
<tr>
<td>RegCounter</td>
<td>Indicates how many times this authenticator has performed registrations in the past.</td>
</tr>
<tr>
<td>PublicKey</td>
<td>User Authentication public key(Uauth.pub) newly generated by authenticator</td>
</tr>
<tr>
<td>signature</td>
<td>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.</td>
</tr>
</tbody>
</table>

Table 18 Key Registration Data

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

Table 19 Signed Data

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:

<table>
<thead>
<tr>
<th>Assurance class</th>
<th>Assurance components</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASE: Security Target evaluation</td>
<td>ASE_INT.1 ST Instruction</td>
</tr>
<tr>
<td></td>
<td>ASE_CCL.1 Conformance claims</td>
</tr>
<tr>
<td></td>
<td>ASE_SPD.1 Security Problem Definition</td>
</tr>
<tr>
<td></td>
<td>ASE_OBJ.2 Security objectives</td>
</tr>
<tr>
<td></td>
<td>ASE_ECD.1 Extended components definition</td>
</tr>
<tr>
<td></td>
<td>ASE_REQ.2 Derived security requirements</td>
</tr>
<tr>
<td></td>
<td>ASE_TSS.1 TOE summary specification</td>
</tr>
<tr>
<td>Development</td>
<td>ADV_ARC.1 Security architecture description</td>
</tr>
<tr>
<td></td>
<td>ADV_FSP.2 Security-enforcing functional specification</td>
</tr>
<tr>
<td></td>
<td>ADV_TDS.1 Basic design</td>
</tr>
<tr>
<td>Guidance documents</td>
<td>AGD_OPE.1 Operational user guidance</td>
</tr>
</tbody>
</table>
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 meets all requirements for content and presentation of evidence.

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.
- 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 enforing 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 one 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.

<table>
<thead>
<tr>
<th>Security Objectives</th>
<th>TOE Security Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>O. Management</td>
</tr>
<tr>
<td>FCO_NRO.1</td>
<td></td>
</tr>
<tr>
<td>FCS_COP.1</td>
<td></td>
</tr>
<tr>
<td>FRN_RNG.1</td>
<td></td>
</tr>
<tr>
<td>FDP_ACC.1(1)</td>
<td></td>
</tr>
<tr>
<td>FDP_ACF.1(1)</td>
<td></td>
</tr>
<tr>
<td>FDP_ACC.1(2)</td>
<td></td>
</tr>
<tr>
<td>FDP_ACF.1(2)</td>
<td></td>
</tr>
<tr>
<td>FIA_AFL.1</td>
<td></td>
</tr>
<tr>
<td>FIA_SOS.1</td>
<td></td>
</tr>
<tr>
<td>FIA_UAU.7</td>
<td></td>
</tr>
<tr>
<td>FIA_UAU.2</td>
<td></td>
</tr>
<tr>
<td>FIA_UID.2</td>
<td></td>
</tr>
<tr>
<td>FMT_MOF.1</td>
<td></td>
</tr>
<tr>
<td>FMT_MSA.1</td>
<td></td>
</tr>
</tbody>
</table>
Table 21 mappings between Security Objectives for the TOE and TOE SFRs

| 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 |

**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, TOE_a, 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, TOE_a, 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_MOI.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.

<table>
<thead>
<tr>
<th>No.</th>
<th>SFRs</th>
<th>Dependencies</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>FRN_RNG.1</td>
<td>none</td>
<td>none</td>
</tr>
<tr>
<td>1</td>
<td>FCS_COP.1</td>
<td>[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]</td>
<td>-</td>
</tr>
</tbody>
</table>
Table 22 Dependencies of SFRs

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

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.
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.

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.

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

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.

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.

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 TOE.

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

<table>
<thead>
<tr>
<th>Terminology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIDO(Fast IDentity Online)</td>
<td>Online user authentication method using device based authentication mechanism, such as fingerprint recognition, iris recognition, or PIN verification.</td>
</tr>
<tr>
<td>FIDO Alliance</td>
<td>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.</td>
</tr>
<tr>
<td>UAF(Universal Authentication Framework)</td>
<td>International standard of authentication method defined by FIDO 1.0</td>
</tr>
<tr>
<td>FIDO UAF Protocol</td>
<td>Communication protocol for FIDO UAF Message between user device and Service Provider</td>
</tr>
<tr>
<td>FIDO Server</td>
<td>Server entity on FIDO UAF protocol side.</td>
</tr>
<tr>
<td></td>
<td>Interacts with SP Web Server to exchange UAF protocol message with FIDO Client</td>
</tr>
<tr>
<td></td>
<td>Inspects trusted authenticator through metadata verification, and evaluates credibility of user authentication and payment transaction information.</td>
</tr>
<tr>
<td>FIDO Client</td>
<td>Software entity which processes UAF protocol message on FIDO user device.</td>
</tr>
<tr>
<td></td>
<td>Communicates with Authenticator through API and communicates with FIDO Server by interacting with users through device interface.</td>
</tr>
<tr>
<td>Admin Portal</td>
<td>Web based Admin page that provides features, such as FIDO Server configuration change, license management, and service history and statistics management.</td>
</tr>
<tr>
<td>Service Provider(Relying Party)</td>
<td>Entity that uses FIDO protocol for user authentication</td>
</tr>
<tr>
<td>SP Server</td>
<td>SP Application that runs on server side and answers to HTTP requests.</td>
</tr>
<tr>
<td>SP App</td>
<td>SP Application built on open web platform that runs on user side.</td>
</tr>
<tr>
<td>ASM (Authenticator Specific Module)</td>
<td>Software that provides API so that FIDO Client can communicate with Authenticator of device.</td>
</tr>
<tr>
<td>Authenticator</td>
<td>Creates Key for FIDO UAF authentication in secured area inside the user device.</td>
</tr>
<tr>
<td>Discovery</td>
<td>Activity of discovering the Authenticator that works with FIDO among authenticators for device.</td>
</tr>
<tr>
<td>Registration</td>
<td>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.</td>
</tr>
<tr>
<td>Authentication</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Transaction Confirmation</strong></td>
<td>Transaction Confirmation happens during Authentication when contents contain confirmation; for example, payment transaction.</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Deregistration</strong></td>
<td>Activity of erasing a public key from FIDO Server and private key from Authenticator.</td>
</tr>
<tr>
<td><strong>PKI (Public Key Infrastructure)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Private Key</strong></td>
<td>Key that only key owner can recognize.</td>
</tr>
<tr>
<td><strong>Public Key</strong></td>
<td>Key that other entity can use</td>
</tr>
<tr>
<td><strong>Attestation Private key</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Attestation Certificate</strong></td>
<td>A public key certificate related to an Attestation Key.</td>
</tr>
<tr>
<td><strong>User’s Private key</strong></td>
<td>This is created by Authenticator during Authentication. User’s Private key is used to sign the authentication data.</td>
</tr>
<tr>
<td><strong>User’s Public Key</strong></td>
<td>This is created by Authenticator during Authentication. User’s Public key is used to verify the digital signature generated by Authenticator.</td>
</tr>
<tr>
<td><strong>Time Stamp</strong></td>
<td>Parameter that indicates specific time frame</td>
</tr>
<tr>
<td><strong>Hash</strong></td>
<td>Algorithm that maps random length of data into certain length of data.</td>
</tr>
<tr>
<td><strong>TLS (Transport Layer Security)</strong></td>
<td>Encryption protocol for TCP/IP network communication which is used for protecting data transmitted between FIDO Server and FIDO Client.</td>
</tr>
<tr>
<td><strong>Biometrics Information</strong></td>
<td>Information based on person’s own and unique body structure and components.</td>
</tr>
<tr>
<td><strong>PIN (personal identification number)</strong></td>
<td>Personal Identification Number which is used to verify identification.</td>
</tr>
<tr>
<td><strong>AAID (Authenticator Attestation ID)</strong></td>
<td>ID that each Authenticator has to identify if UAF can authenticate. AAID is composed of Authenticator manufacturer information and model information.</td>
</tr>
<tr>
<td><strong>API Key</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>AppID</strong></td>
<td>URL indicating TrustedFacet List (FacetID) by RP.</td>
</tr>
<tr>
<td><strong>FacetID</strong></td>
<td>OS/Platform Identifier for cases where one SP App is on several different OS/Platforms.</td>
</tr>
<tr>
<td><strong>FacetList</strong></td>
<td>List data architecture for FacetID, and AppID is used to have this architecture</td>
</tr>
<tr>
<td><strong>KeyID</strong></td>
<td>ID to identify UAuth.Key that is created by Authenticator.</td>
</tr>
<tr>
<td><strong>ServerChallenge</strong></td>
<td>Random value produced by FIDO Server, which is used for verifying response message that FIDO Server received.</td>
</tr>
<tr>
<td><strong>FinalChallenge</strong></td>
<td>Data created in FIDO client using value of AppID, challenge, facetID, channelBinding</td>
</tr>
<tr>
<td><strong>License</strong></td>
<td>Certificate that product manufacturer produces to protect the product information. Through license verification process, only authorized SP Server works for FIDO</td>
</tr>
<tr>
<td><strong>Metadata</strong></td>
<td>Data of authorized Authenticator</td>
</tr>
<tr>
<td><strong>Policy</strong></td>
<td>JSON data architecture used for transmitting data, such as Authenticator specification or information, to FIDO Client when operating FIDO</td>
</tr>
<tr>
<td><strong>SecurityWarning</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>BlackList</strong></td>
<td>Blacklist extracts problematic users from Security Warning and manages them on a blacklist to avoid further problems</td>
</tr>
<tr>
<td><strong>Delivery Manager</strong></td>
<td>Deploys and installs TOE based on the installation manual.</td>
</tr>
<tr>
<td><strong>Operation Administrator</strong></td>
<td>Group of users who can manage user data, license, SP, Metadata, and check service history and statistics of FIDO through Admin Portal.</td>
</tr>
<tr>
<td><strong>Operator</strong></td>
<td>Group of users who can check service history and statistics of FIDO through Admin Portal.</td>
</tr>
</tbody>
</table>
Reference

[1] FIDO Technical Glossary


[3] FIDO UAF Architectural Overview

[4] FIDO UAF Registry of Predefined Values

[5] FIDO UAF Authenticator Metadata Statements v1.0


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