KECS-CR-15-73

SAMSUNG SDS FIDO Server Solution V1.1

Certification Report

Certification No.: KECS-ISIS-0645-2015

2015. 9. 10

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2015.09.09	-	Certification report for SAMSUNG SDS FIDO Server Solution V1.1 - First documentation

This document is the certification report for SAMSUNG SDS FIDO Server Solution V1.1.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea Testing Certification (KTC)

Table of Contents

1. Executive Summary

This report describes the certification result drawn by the certification body on the results of the EAL2 evaluation of SAMSUNG SDS FIDO Server Solution V1.1 with reference to the Common Criteria for Information Technology Security Evaluation (“CC” hereinafter) [1]. It describes the evaluation result and its soundness and conformity.

The Target of Evaluation (TOE) is software consisting of authentication server (FIDO Server) which authenticates users in accordance with FIDO UAF protocol server requirements by FIDO Alliance [5], and security management (FIDO Admin Portal).

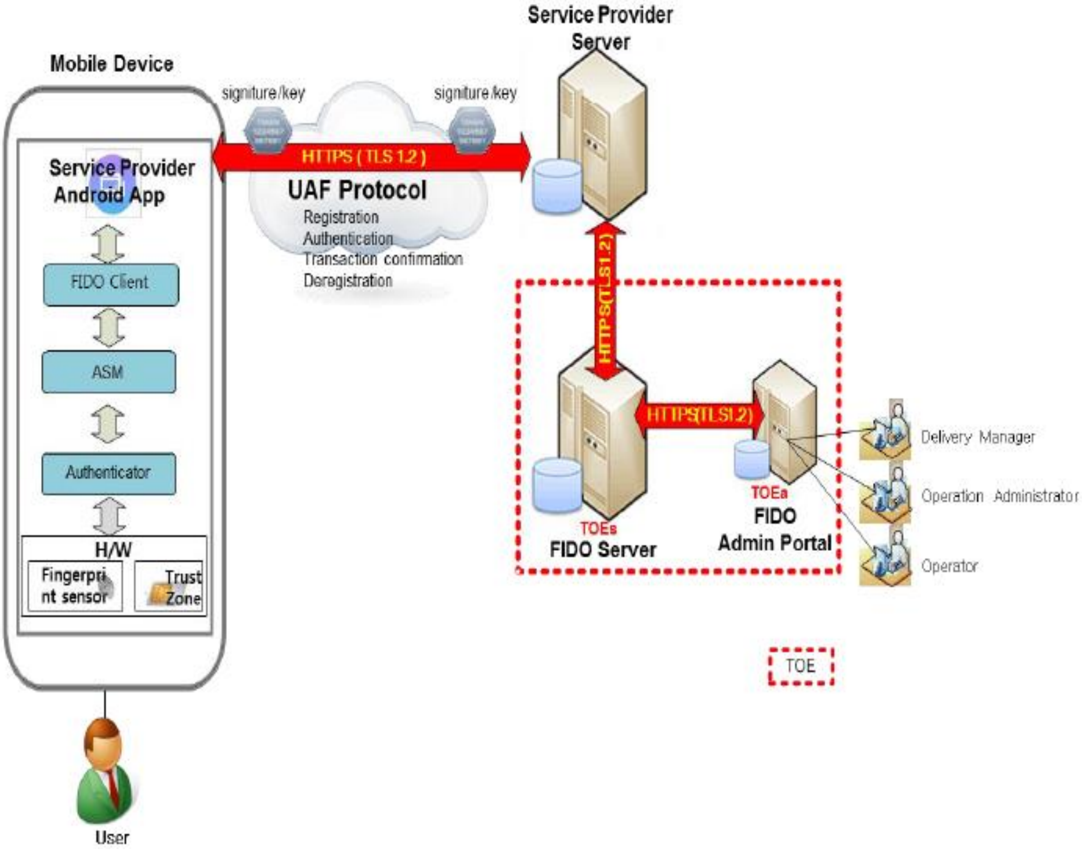
The TOE SAMSUNG SDS FIDO Server Solution V1.1 is composed of the following components:

- SDS FIDO Server V1.1.1 (12), and
- SDS FIDO Admin Portal V1.1.1 (12).

The evaluation of the TOE has been carried out by Korea Testing Certification (KTC) and completed on September 4, 2015. This report grounds on the evaluation technical report (ETR) KTC had submitted [6] and the Security Target (ST) [7][8].

The ST does not claim conformance to a Protection Profile. All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL2. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon both functional components in CC Part 2 and a newly defined component in the Extended Component Definition chapter of the ST, and the TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 extended.

[Figure 1] shows the operational environment of the TOE. FIDO Server communicates with FIDO Client in accordance with FIDO UAF Protocol Specification V1.0 [5] based on the public key cryptography. The mobile device embeds FIDO Client, ASM (Authenticator-Specific Module), and Authenticator necessary for the TOE, and must ensure the secure protection of the private key stored in it. The user of the mobile device can be authenticated by the TOE (i.e., FIDO Server) when the user tries to access services which require user authentication prior to use such as on-line banking and e-commerce through Service Provider’s App and Server. Also, the Service Provider’s App and Server developers must comply with FIDO UAF Protocol Specification V1.0 [5] to communicate with the TOE (i.e., FIDO Server).



[Figure 1] Operational environment of the TOE

The TOE provides security features to authenticate users providing countermeasures against attacks including replaying attack, transmitted data forgery attack, Authenticator cloning attack.

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE is software consisting of the following components and related guidance documents.

Type	Identifier	Version	Delivery Form
SW	SDS FIDO Server	V1.1.1 (12)	CD
	SDS FIDO Admin Portal	V1.1.1 (12)	
DOC	FIDO_Manager Manual_V1.1_Kor	V1.1	CD (Softcopy)
	FIDO_Install Manual_V1.1_Kor	V1.1	
	FIDO_User Manual_V1.1_Kor	V1.1	
	FIDO_Application Developer Manual(Server)_V1.1_Kor	V1.1	
	FIDO_Application Developer Manual(Client)_V1.1_Kor	V1.1	

[Table 1] TOE identification

[Table 2] summarizes additional information for scheme, developer, sponsor, evaluation facility, certification body, etc..

Scheme	Korea Evaluation and Certification Guidelines for IT Security (August 8, 2013) Korea Evaluation and Certification Scheme for IT Security (November 1, 2012)
TOE	SAMSUNG SDS FIDO Server Solution V1.1 – SDS FIDO Server V1.1.1 (12) – SDS FIDO Admin Portal V1.1.1 (12)
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL2
Developer	Samsung SDS
Sponsor	Samsung SDS
Evaluation Facility	Korea Testing Certification (KTC)
Completion Date of Evaluation	September 4, 2015
Certification Body	IT Security Certification Center

[Table 2] Additional identification information

3. Security Policy

The ST [7][8] for the TOE states that the TOE provides FIDO Server's security features defined in FIDO UAF Specifications [5], and FIDO Admin Portal's security features to securely manage the TOE itself as follows:

- Digital signature verification to authenticate users in accordance with the following list of cryptographic algorithms,
  - UAF_ALG_SIGN_SECP256R1_ECDSA_SHA256_RAW
  - UAF_ALG_SIGN_SECP256R1_ECDSA_SHA256_DER
  - UAF_ALG_SIGN_SECP256K1_ECDSA_SHA256_RAW
  - UAF_ALG_SIGN_SECP256K1_ECDSA_SHA256_DER
  - UAF_ALG_SIGN_RSASSA_PSS-SHA256_RAW
  - UAF_ALG_SIGN_RSASSA_PSS-SHA256_DER
- Pseudo random generation for protection of integrity of the transmitted data,
- Access control to the Service Provider Server, Authenticator, and FIDO Admin Portal,
- Identification and authentication of authorized administrators,
- Security management of users, administrators, security policies, etc, and
- Audit data generation in case of auditable events.

For more details refer to the the ST [7][8].

4. Assumptions and Clarification of Scope

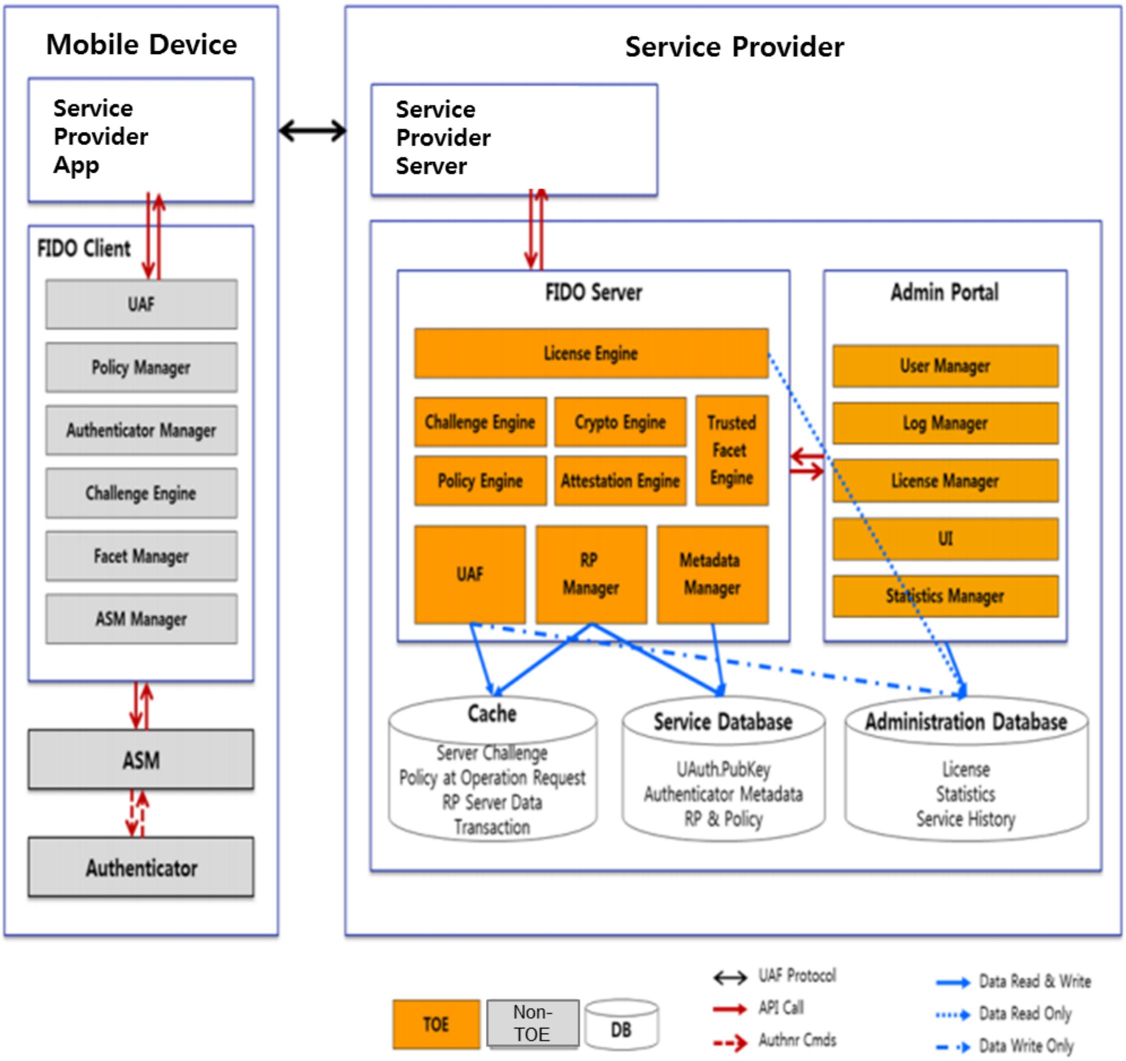
The following assumptions describe the security aspects of the operational environment in which the TOE will be used or is intended to be used (for the detailed and precise definition of the assumption refer to the ST [7][8], chapter 3.3):

- The secure element or trusted execution environment in the mobile device provide secure storage for the private key generated by the authenticator.
- The Service Provider's App and Server developers must comply with FIDO UAF Protocol Specification V1.0 [5] to communicate with the TOE (i.e., FIDO Server).
- The mobile device user uses reliable Service Provider's App, FIDO Client, ASM and Authenticator in the device.

For the complete list of assumptions regarding the operational environment of the TOE, refer to the ST [7][8], chapter 3.3. Furthermore, some aspects of threats and organisational security policies are not covered by the TOE itself, thus these aspects are addressed by the TOE environment. Details can be found in the ST [7][8], chapter 3.1, 3.2 and 4.2.

5. Architectural Information

[Figure 2] shows architecture of the TOE. The TOE is software which is consisting of the FIDO Server and FIDO Admin Portal.



[Figure 2] Architecture of the TOE

- FIDO Server provides security features of digital signature verification to authenticate users, pseudo random generation for protection of integrity of the transmitted data, and access control to the Service Provider Server, Authenticator, and FIDO Admin Portal.
- FIDO Admin Portal provides security features of identification and authentication of authorized administrators, security management to the TOE and TSF data, audit data generation in case of auditable events for both FIDO Server and FIDO Admin Portal, and access control to the FIDO Admin Portal itself.

For the detailed description is referred to the ST [7][8].

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Version	Date
FIDO_Manager Manual_V1.1_Kor	V1.1	August 21, 2015
FIDO_Install Manual_V1.1_Kor	V1.1	August 25, 2015
FIDO_User Manual_V1.1_Kor	V1.1	July, 2015
FIDO_Application Developer Manual(Server)_V1.1_Kor	V1.1	April, 2015
FIDO_Application Developer Manual(Client)_V1.1_Kor	V1.1	April, 2015

[Table 3] Documentation

7. TOE Testing

The developer took a testing approach based on the SFRs defined in the ST [7][8] and TSFIs, using tools such as debugging tools and the developer’s in-house simulator:

- SFRs tests, testing the correct implementation of the Security Functional Requirements described in the ST.
- TSFIs tests, testing the functionality invoked using TSFIs.

The developer tested all the TSF and analyzed testing results according to the assurance component ATE_COV.1. This means that the developer tested all the TSFI defined for SFR-enforcing of the TOE, and demonstrated that the TSFI behaves as described in the functional specification.

The developer correctly performed and documented the tests according to the assurance component ATE_FUN.1.

The evaluator performed all tests provided by developer and conducted independent testing based upon test cases devised by the evaluator. The TOE and test configuration are identical to the developer's tests. The tests cover preparative procedures, according to the guidance.

Also, the evaluator conducted vulnerability analysis and penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities.

The evaluator's testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [6].

8. Evaluated Configuration

The TOE is SAMSUNG SDS FIDO Server Solution V1.1 consisting of the following components:

- SDS FIDO Server V1.1.1 (12), and
- SDS FIDO Admin Portal V1.1.1 (12).

Administrator can identify the complete TOE reference after logging in FIDO Server and FIDO Admin Portal. And the guidance documents listed in chapter 6 of this report, [Table 3] were evaluated with the TOE.

For details regarding non-TOE hardware/software/firmware required by the TOE, refer to the evaluated guidance documents.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [6] which references Work Package Reports for each assurance requirement and Observation Reports.

The evaluation result was based on the CC [1] and CEM [2].

As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL2.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.

The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.

The Security Problem Definition clearly defines the security problem intended to be addressed by the TOE and its operational environment. Therefore the verdict PASS is assigned to ASE_SPD.1.

The Security Objectives adequately and completely address the security problem definition and the division of this problem between the TOE and its operational environment is clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.2.

The Extended Components Definition has been clearly and unambiguously defined, and it is necessary. Therefore the verdict PASS is assigned to ASE_ECD.1.

The Security Requirements is defined clearly and unambiguously, and it is internally consistent and the SFRs meet the security objectives of the TOE. Therefore the verdict PASS is assigned to ASE_REQ.2.

The TOE Summary Specification addresses all SFRs, and it is consistent with other narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer uses a CM system that uniquely identifies all configuration items. Therefore the verdict PASS is assigned to ALC_CMC.2.

The configuration list includes the TOE, the parts that comprise the TOE, and the evaluation evidence. These configuration items are controlled in accordance with CM capabilities. Therefore the verdict PASS is assigned to ALC_CMS.2.

The delivery documentation describes all procedures used to maintain security of the TOE when distributing the TOE to the user. Therefore the verdict PASS is assigned to ALC_DEL.1.

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include the configuration management used throughout TOE development and the delivery activity.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The TOE design provides a description of the TOE in terms of subsystems sufficient to determine the TSF boundary. Therefore the verdict PASS is assigned to ADV_TDS.1.

The developer has provided a description of the TSFIs in terms of their purpose, method of use, and parameters. In addition, for the SFR-enforcing TSFIs the developer has described the SFR-enforcing actions and direct error messages. Therefore the verdict PASS is assigned to ADV_FSP.2.

The TSF is structured such that it cannot be tampered with or bypassed, and TSFs that provide security domains isolate those domains from each other. Therefore the verdict PASS is assigned to ADV_ARC.1.

Thus, the design documentation is adequate to understand how the TSF meets the SFRs and how the implementation of these SFRs cannot be tampered with or bypassed. Design documentation consists of a functional specification (which describes the interfaces of the TSF), a TOE design description (which describes the architecture of the TSF in terms of how it works in order to perform the functions related to the SFRs being claimed). In addition, there is a security architecture description (which describes the architectural properties of the TSF to explain how its security enforcement cannot be compromised or bypassed).

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

The developer has tested TSFIs, and that the developer's test coverage evidence shows correspondence between the tests identified in the test documentation and the TSFIs described in the functional specification. Therefore the verdict PASS is assigned to ATE_COV.1.

The developer correctly performed and documented the tests in the test documentation. Therefore the verdict PASS is assigned to ATE_FUN.1.

By independently testing a subset of the TSF, the evaluator confirmed that the TOE behaves as specified in the design documentation, and had confidence in the developer's test results by performing all of the developer's tests. Therefore the verdict PASS is assigned to ATE_IND.2.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.2.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE, don’t allow attackers possessing basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_SPD.1	ASE_SPD.1.1E	PASS	PASS	
	ASE_OBJ.2	ASE_OBJ.2.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.2	ASE_REQ.2.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.2	ALC_CMS.2.1E	PASS	PASS	PASS
	ALC_CMC.2	ALC_CMC.2.1E	PASS	PASS	
	ALC_DEL.1	ALC_DEL.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS
		AGD_PRE.1.2E	PASS	PASS	
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_TDS.1	ADV_TDS.1.1E	PASS	PASS	PASS
		ADV_TDS.1.2E	PASS	PASS	
	ADV_FSP.2	ADV_FSP.2.1E	PASS	PASS	
		ADV_FSP.2.2E	PASS		
	ADV_ARC.1	ADV_ARC.1.1E	PASS	PASS	
ATE	ATE_COV.1	ATE_COV.1.1E	PASS	PASS	PASS
	ATE_FUN.1	ATE_FUN.1.1E	PASS	PASS	
	ATE_IND.2	ATE_IND.2.1E	PASS	PASS	
		ATE_IND.2.2E	PASS		
		ATE_IND.2.3E	PASS		
AVA	AVA_VAN.2	AVA_VAN.2.1E	PASS	PASS	PASS
		AVA_VAN.2.2E	PASS		
		AVA_VAN.2.3E	PASS		
		AVA_VAN.2.4E	PASS		

[Table 4] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- While the TOE consists of FIDO Server and FIDO Admin Portal, Authenticator/ ASM/FIDO Client shall be preloaded in the mobile device, and Service Provider’s App and Server shall communicate each other in accordance with the FIDO UAF protocol specification.
- Service Provider’s App and Server shall be developed by the service provider in accordance with the FIDO Application Developer Manual for both Server and Client provided by Samsung SDS, and the FIDO UAF protocol specification.
- Although FIDO Server supports 6 kinds of algorithms for digital signature verification, it depends on the mobile device for which algorithm is used.
- In accordance with the FIDO UAF protocol specification, TLS1.2 is used for communication between the mobile device and Service Provider’s Server as well as between Service Provider’s Server and FIDO Server. Upon use of TLS1.2, the secure algorithm shall be used for secure communication.
- Service Provider shall ensure security of Service Provider’s Server to protect information related to Authenticators and public keys.
- For FIDO UAF authentication, the mobile device shall provide secure storage such as Trusted Execution Environment (TEE) for secure information such as private keys.

11. Security Target

The SDS FIDO V1.1 Security Target V2.0, September 2, 2015 [7] is included in this report by reference. For the purpose of publication, it is provided as sanitized version [8] according to the CCRA supporting document ST sanitising for publication [9].

12. Acronyms and Glossary

ASM	Authenticator-Specific Module
CC	Common Criteria
FIDO	Fast IDentity Online
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
UAF	Universal Authentication Framework

ASM Software that provides API so that FIDO Client can communicate with Authenticator of device.

Authenticator Creates Key for FIDO UAF authentication in secured area inside the user device.

FIDO Online user authentication method using device based authentication mechanism, such as fingerprint recognition, iris recognition, or PIN verification.

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

FIDO Client Software entity which processes UAF protocol message on FIDO user device. Communicates with Authenticator through API and communicates with FIDO Server by interacting with users through device interface.

FIDO Server Server entity on FIDO UAF protocol side. Interacts with SP Web Server to exchange UAF protocol message with FIDO Client Inspects trusted authenticator through metadata verification, and evaluates credibility of user

	authentication and payment transaction information.
FIDO UAF Protocol	Communication protocol for FIDO UAF Message between user device and Service Provider
Private Key	Key that only key owner can recognize.
Public Key	Key that other entity can use.
Service Provider App	Service Provider’s Application built on open web platform that runs on user side.
Service Provider	Entity that uses FIDO Protocol for user authentication
Service Provider Server	Service Provider’s Application that runs on server side and answers to HTTP requests.
UAF	International standard of authentication method defined by FIDO 1.0

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
Part 1: Introduction and general model
Part 2: Security functional components
Part 3: Security assurance components

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-004, September 2012

[3] Korea Evaluation and Certification Guidelines for IT Security, August 8, 2013

[4] Korea Evaluation and Certification Scheme for IT Security, November 1, 2012

[5] FIDO UAF Specifications, December 8, 2014

[6] [CC2015-002] SAMSUNG SDS FIDO Server Solution V1.1 Evaluation Technical Report V2.0, September 8, 2015

[7] SDS FIDO V1.1 Security Target V2.0, September 2, 2015 (Confidential Version)

[8] SDS FIDO V1.1 Security Target Lite V2.0, September 2, 2015 (Sanitized Version)

[9] ST sanitising for publication, CCDB-2006-04-004, April 2006