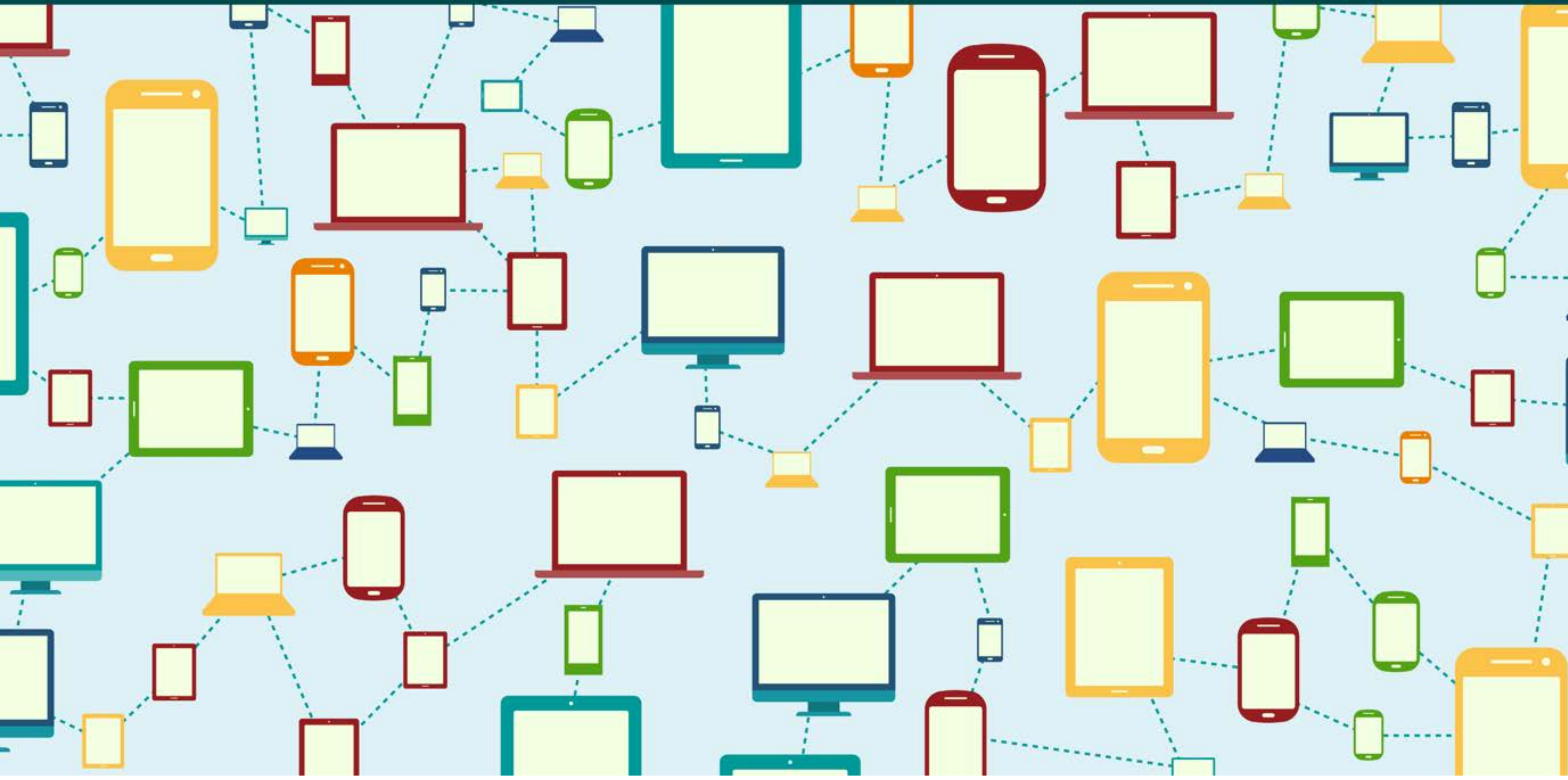


FIDO Alliance White Paper: Korean FIDO Deployment Case Study- Accredited Certification System for Safe Usage of Accredited Certificate using FIDO in Smartphone in Korea (K-FIDO)

Editor: Dr. Jaejung Kim, KICA (Korea information Certificate Authority)

Table of Contents

Abstract

To date, Korea is one of the most advanced countries where FIDO has been successfully deployed for various financial services nationwide. Korea had successfully deployed nationwide national ID and accredited certificates for online businesses before FIDO came out. This paper describes a case study introducing how “K-FIDO” combines FIDO UAF specification and PKI to enable authentication and ID verification at the same time for successful commercial Fintech deployments in Korea. K-FIDO is a specification to be published by KISA (Korea Internet Security Agency), enabling biometric accredited certification services that provide accredited certificates without password using FIDO in Korea. This paper, after introducing the Korean national ID and Accredit CA as the enabler for identity management in the background, describes the details of K-FIDO that combines FIDO UAF and PKI to enable authentication, identify verification and interoperability among various Fintech services for increased user convenience.

This is a white paper that Deployment at Scale (D@S) WG of FIDO Alliance has developed.

1. Introduction

Formed in July 2012, the FIDO Alliance aims at changing the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that reduce reliance on passwords and support strong and convenient user authentication to online services. The FIDO protocols use standard public key cryptography techniques to provide stronger authentication. The FIDO UAF protocol [1] consists of registration, authentication, transaction confirmation, and deregistration. The FIDO registration process is as follows: First, the User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy. Second, User unlocks the FIDO authenticator using some user gesture such as swiping a fingerprint reader, pressing a button on a second–factor device, securely entering a PIN or using some other method. Third, the User's authenticator creates a new public/private key pair unique for the authenticator, the online service and user's account. Fourth, the public key is sent to the online service 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. FIDO registration assumes a prior identity-binding step in order to know the identity of the authenticator owner.

The authentication process is as follows; First, Online service challenges the user to authenticate with a previously registered authenticator that matches the service's acceptance policy. Second, User unlocks the FIDO authenticator using the same method as at Registration time. Third, the authenticator uses the user's account identifier provided by the service to select the correct key and signs the challenge that is sent from the service, using the private key. Fourth, the authenticator generates the signed challenge, which is returned back to the service and verified using the stored public key.

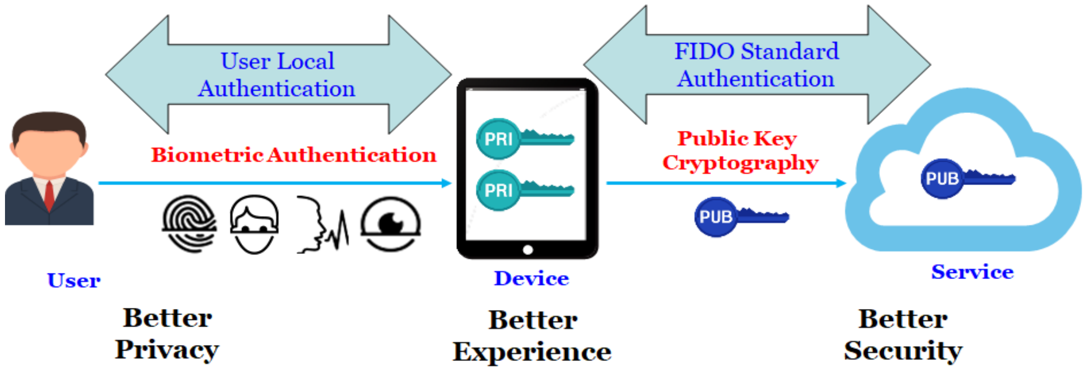


Figure 1. FIDO UAF Architecture.

Digital certificates are one of the many solutions available for electronic identification, secure email communication, document signing and authentication, but they are easy to copy and leak. Mobile services need to properly manage registered devices and users, and require trusted means of authenticating their users. Many online and mobile apps are used to manage highly valuable data, such as financial transactions, personally identifiable information (PII) or intellectual property. It is vital therefore to secure access to these apps through strong authentication.

2. Korean national ID and Accredit CA as background

2.1. National ID and i-PIN (internet-Personal Identification Number)

National ID is used in offline identification and i-PIN is used in online because the national ID contains very sensitive personal information such as birthday, gender, birth area code, etc.

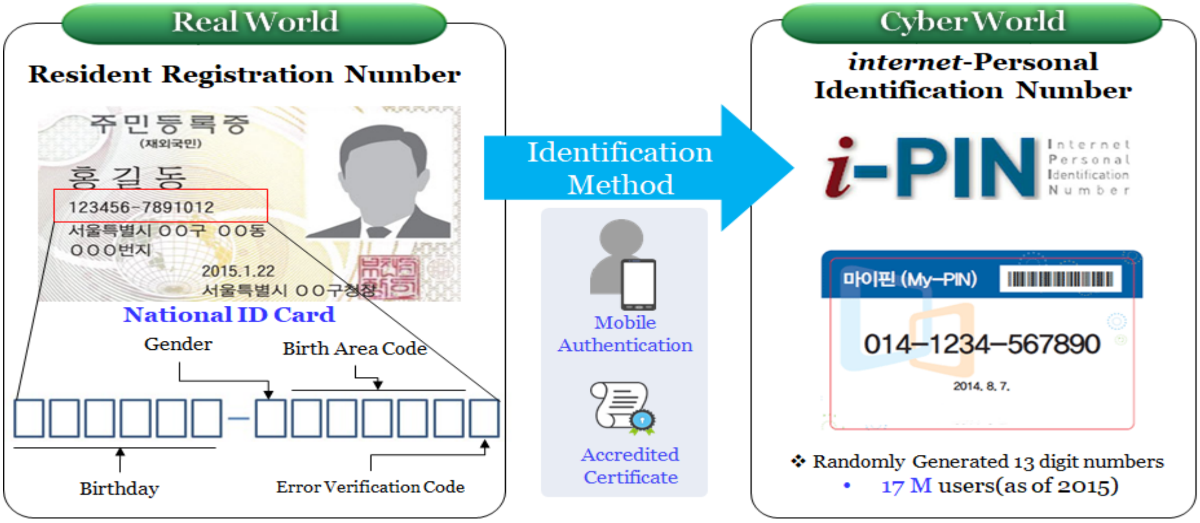


Figure 2. National ID and i-PIN in Korea.

2.1.1. Resident's Registration Number (National ID)

- According to UN E-Government Survey 2016, Republic of Korea (Korea) is one of the most advanced country for e–Government Development.
- UN E-Government Survey rated Korea No 1 for E–Government Development Index in 2010, 2012, and 2014 (survey conducted every 2 years)
- Every Korean resident is assigned a 13 digit Resident's Registration Number (주민등록번호)(住民登□番□), similar to National Identification Numbers in other countries.
- A Resident's Registration Number is used to identify people in various private transactions, e.g., banking and employment. It is also used extensively for online identification purposes.
- A resident registration card is issued to a resident at the age of 17 years

- By the Korean law, Privacy Protection ACT, anyone is prohibited to collect Resident's Registration Numbers except for the Accredit CAs (5CAs permitted), Telecom Companies, Banks, i-PIN Service Providers, etc.

2.1.2. i-PIN (Internet-Personal Identification Number)

- In order to solve Internet security problems and promote online business based on the National PKI system, i-PIN (Internet Personal Identification Number) is widely used in Korea as an online identity since 2006.
- A Resident's Registration Number or a National ID cannot be changed and it may be vulnerable for security problems if it is used in the Internet.
- An i-PIN is bound to a user's Resident's Registration Number and only one i-PIN is assigned to a user at a time, but it can be changed. Thus, it is more suitable for online authentication than a Resident's Registration Number, or a National ID, that cannot be changed.
- A user may ask i-PIN Service Providers to issue an i-PIN by presenting his/her Accredit Certificate or mobile authentication from Telco companies.
- There are 4 i-PIN Service Providers.
  - Siren 24 i-PIN by Seoul Credit Rating & Information, KCB i-PIN by the Korea Credit Bureau, Nice i-PIN by Information & Credit Evaluation, Public i-PIN by the Ministry of the Interior(MOI)
- Users are able to create and register Web accounts using i-PINs as their identities.
- Sometimes a 13-digit Resident's Registration Number, or a National ID, is called as a "physical ID" while an i-PIN is called as an "online ID".

2.2. Identification Method

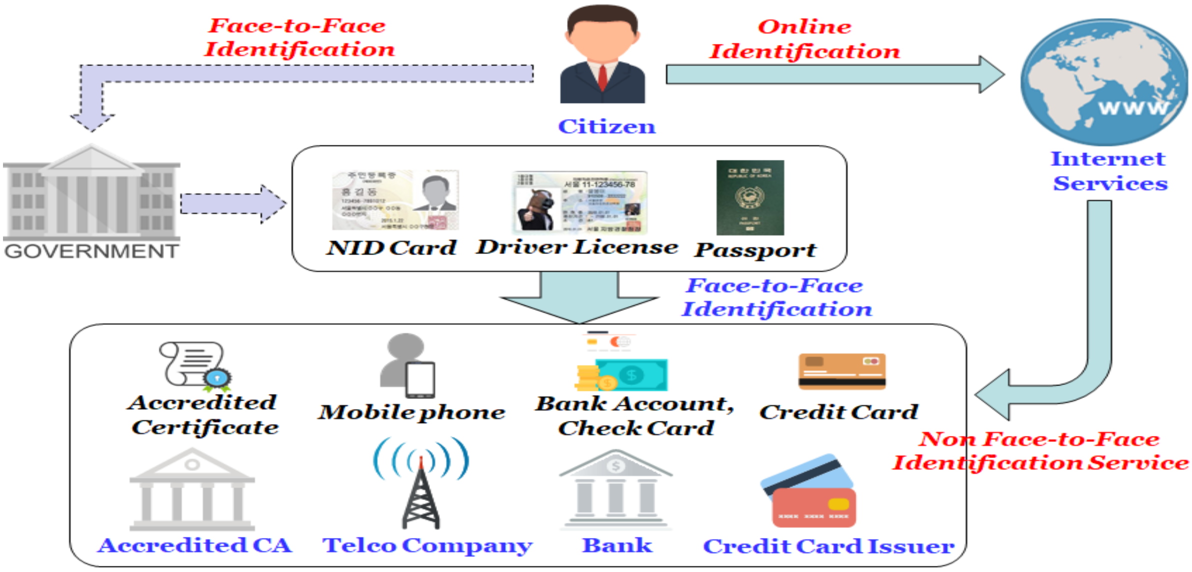


Figure 3. Online and offline identification method in Korea.

The citizen can use many identification methods such as accredited certificates, mobile, bank accounts, and credit cards for internet services that request an online (i.e. non face-to-face) identification method.

Online service providers can choose Identification methods such as Accredited Certificates, Mobile Authentication, i-PIN, K-FIDO, or FIDO depending on the required authentication levels of assurance.

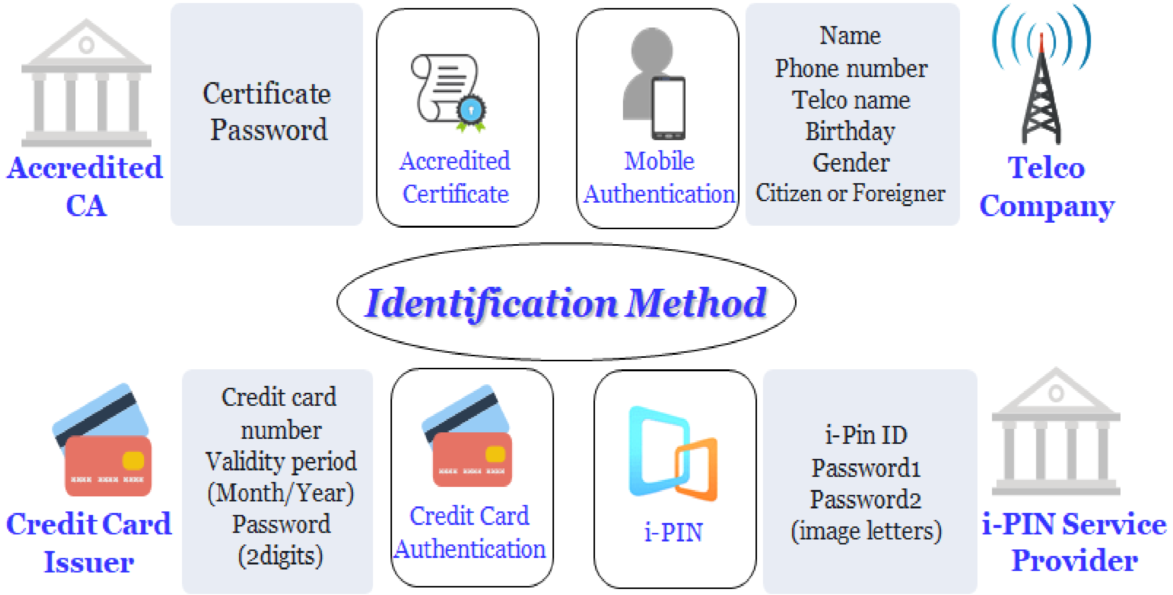
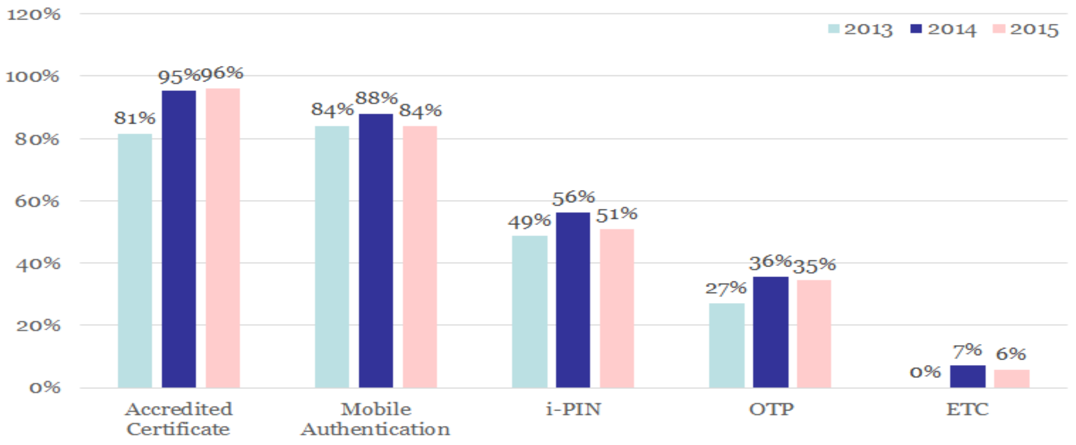


Figure 4. Type of Online Identification Methods.

The use rate of identification method is as follows; the identification methods are used in the order of accredited certificate, mobile authentication, i-PIN, OTP, and so on.

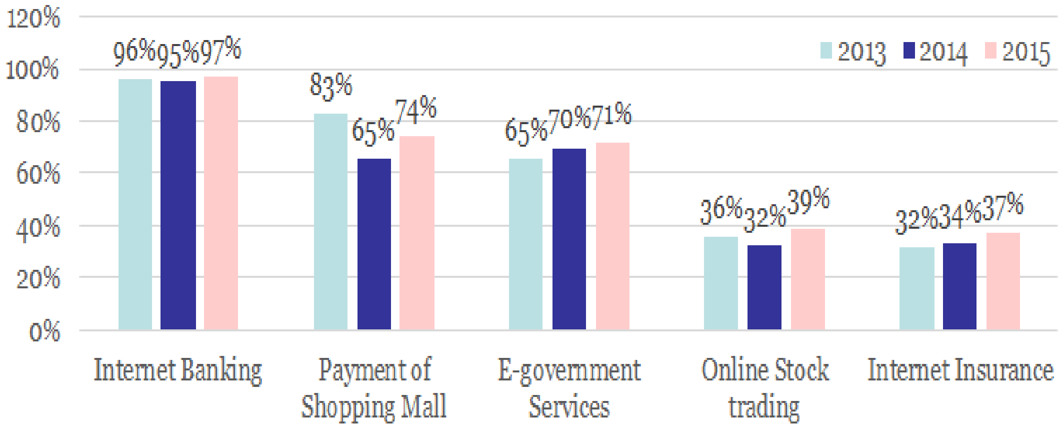


(Source: Research on the Actual Condition of Electronic Signature System Usage(in Electronic Signature User)-KISA, December 2015)

Figure 5. The Use Rate of Identification Method in Korea.

2.2.1. Accredited CAs and Accredited Certificate

- A user may apply for Accredit Certificates from Accredit CAs.
- Accredited Certificates with their private keys can be used for 1) user authentication and 2) electric signature of the user for various uses.
- Korean people typically have several Accredited certificates from different Accredit CAs. For example, one for banks and one for stock markets. If a user has a general purpose accredited certificate he/she can use a lot of applications by one certificate.
- A user must provide his/her certificate issued by the government such as National ID Card, driver license card, passport to an Accredited CA for identification purposes to get an Accredited Certificate. These IDs have the same Resident's Registration Number on it.
- There are only 5 Accredited CAs that are regulated by the Ministry of Science, ICT and Future Planning (MSIP).
  - KICA, KOSCOM, KFTC, CrossCert, and KTNET
- KISA (Korea Internet & Security Agency) defines and publishes standardization of National PKI such as storage of Accredited Certificates including the private keys in local devices, and National PKI is being operated subject to the KISA's specifications.
- KISA as the Root CA in Korea provides the Root CA certificate for the accredited certificates that are issued by the 5 Accredited CAs.
- The top 5 accredited certificate applications are Internet banking, payment at a internet shopping mall, e-government services, online stock trading, and Internet insurance.



(Source: Research on the Actual Condition of Electronic Signature System Usage(in Electronic Signature User)-KISA, December 2015)

Figure 6. Accredited Certificate Applications- Top5.

- 35 million accredited certificates have been issues for the total population of 51 million. Accredited certificates have been available since 2000.

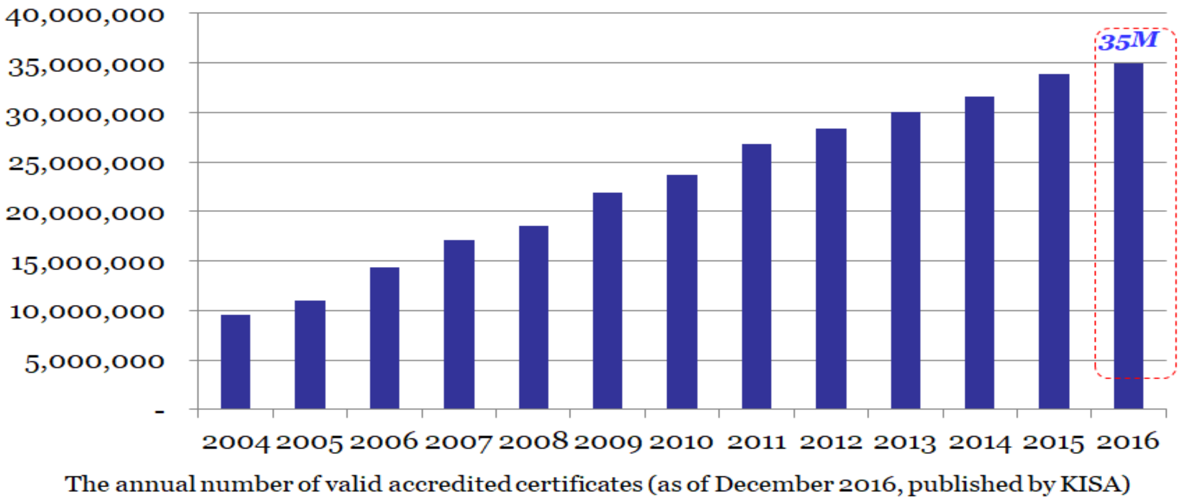


Figure 7. Statistics of Accredited Certificates in Korea.

2.2.2. Mobile Authentication

Mobile Authentication can be used for authentication to web sites, adult authentication, game sites, and financial services, etc.

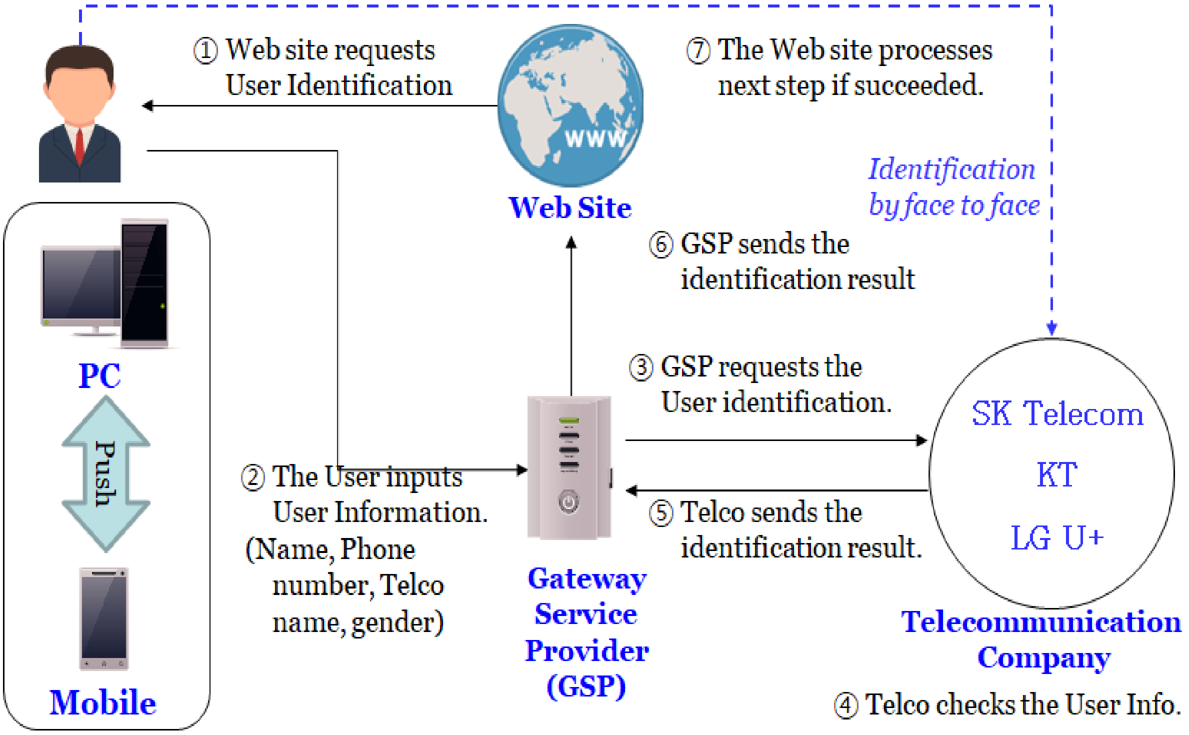

① Web site requests User Identification
⑦ The Web site processes next step if succeeded.
Web Site
Identification by face to face
⑥ GSP sends the identification result
PC
Push
Mobile
③ GSP requests the User identification.
② The User inputs User Information. (Name, Phone number, Telco name, gender)
⑤ Telco sends the identification result.
SK Telecom
KT
LG U+
Gateway Service Provider (GSP)
Telecommunication Company
④ Telco checks the User Info.

Figure 8. Mobile Authentication Process in Korea.

2.3. User Authentication for Various Services

Various user authentication methods used for user authentication for web portals, e-transactions, financial institutions and e-government services are typically supported.

Table 1. User Authentication Methods.

Service	Function		Types of Authentication Methods
Web portal	Log-in (optional)		ID/Password, OTP
	Registration		Mobile phone authentication
	ID/password retrieval (one selected)		Registered mobile phone, User authentication through mobile phone
E-transaction	Log-in		ID/Password or Accredited certificate
	Electronic payment	Account transfer	Account information + Accredited certificate
		Credit card payment	Credit card information + Accredited certificate - VISA Anshim Click, Internet Secure Payment (ISP)
			Mobile phone authentication(+ Fintech Technology)
		Mobile phone payment	Mobile phone authentication
Financial institution (Internet banking)	Log-in		Accredited certificate or ID/PW
	Account transfers	Type 1	Accredited certificate + OTP generator(H/W)
			PKI token(Accredited certificate) + security card
		Type 2	Accredited certificate + security card (+ 2-channel authentication)
		Type 3	Mobile phone authentication(+ Fintech Technology)
Public Procurement Service	Log-in Electronic bidding		Accredited certificate + fingerprint security token

3. How Accredit CA works with FIDO (K-FIDO)

3.1. Background

FIDO focuses on ensuring user privacy as a standard for a horizontal authentication protocol. This is a very important focus for an authentication protocol to be successfully adopted by various vertical services and applications. For example, “When a User registers a FIDO Authenticator for use with a Relying Party, a unique pair of cryptographic keys is produced by the FIDO Authenticator for use solely with that Relying Party. As a result, a User has a different credential for each Relying Party. This means that Relying Parties cannot collude to track a User’s activity online.” [5]. Isolation of RPs is a critical issue from user’s privacy.

User identity is out of the scope of FIDO protocols, since FIDO is an authentication protocol. As such, when registered, FIDO only confirms the match between pre–enrolled biometric data, e.g., fingerprint, and the one on the process. FIDO does not verify the person’s identity, and it must work with other mechanisms if identification is required for the system to be deployed (identity binding). The identification assurance level depends generally on the vertical and the region. Cloud storage providers typically have little or even no requirements on identity binding. When deploying FIDO for other services, however, there are many services that require a strong identity binding. In many financial services, for example, it is important to ensure that the identity of the user who is authenticating is truly the one that the user claims it to be. Typically this is even regulated strictly by the respective Government. From such a perspective, the following issues were identified when deploying FIDO in Korea where a PKI based personal ID system had already been widely deployed and registration of real identity to online services is a legal requirement. It is shown how K-FIDO complemented the issues by introducing extensions to FIDO UAF and combined FIDO UAF and PKI within the framework of UAF Extensions, for a successful nationwide commercial deployment.

3.1.1. Limitation of FIDO (Fast Identity Online) based service

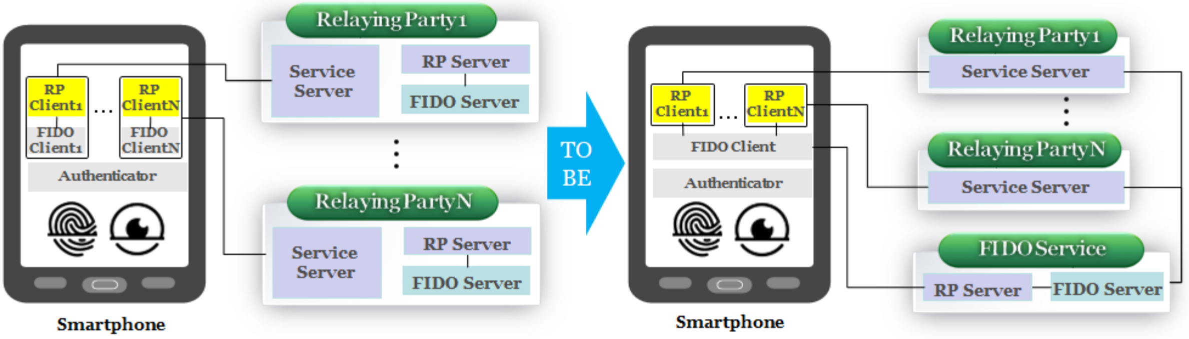


Figure 9. Isolation vs. Interoperability of services.

FIDO requires a user to register his/her authenticator at each site to use the respective service. This is to ensure user privacy [5]. However, as a consequence of this isolation, it by itself doesn't provide an identity binding that is visible across the services.

3.1.2. The verification of person's identity in FIDO

When registered, FIDO only confirms the match between pre–enrolled user verification reference data set (e.g. a fingerprint) and the one provided by the user at authentication time. In other words, FIDO doesn't verify the person's identity. If the user has registered someone else's fingerprint, he or she can precede the FIDO registration instead of the user. In this case, the whole responsibility is placed on the smartphone user. Therefore, it might require additional user ID confirmation if more thorough verification is needed.

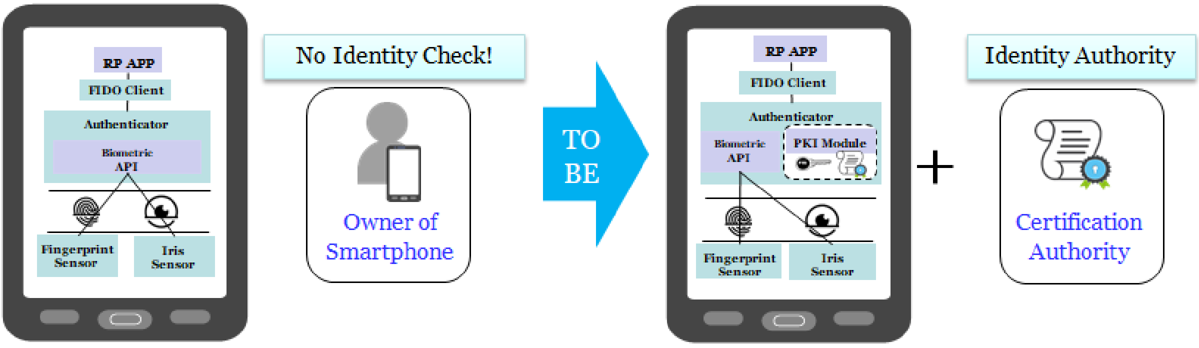
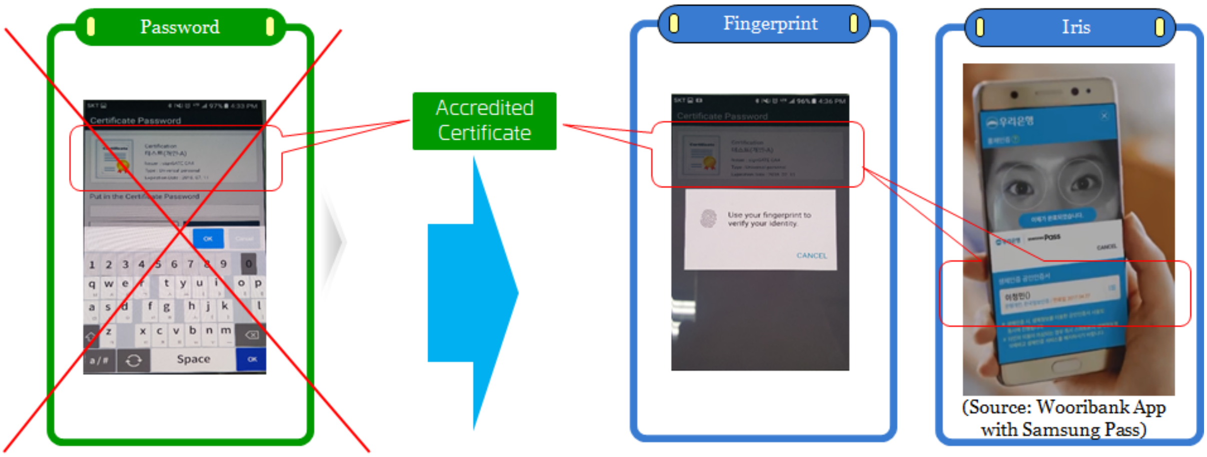


Figure 10. Authentication only vs authentication plus identity.

3.2. Overview

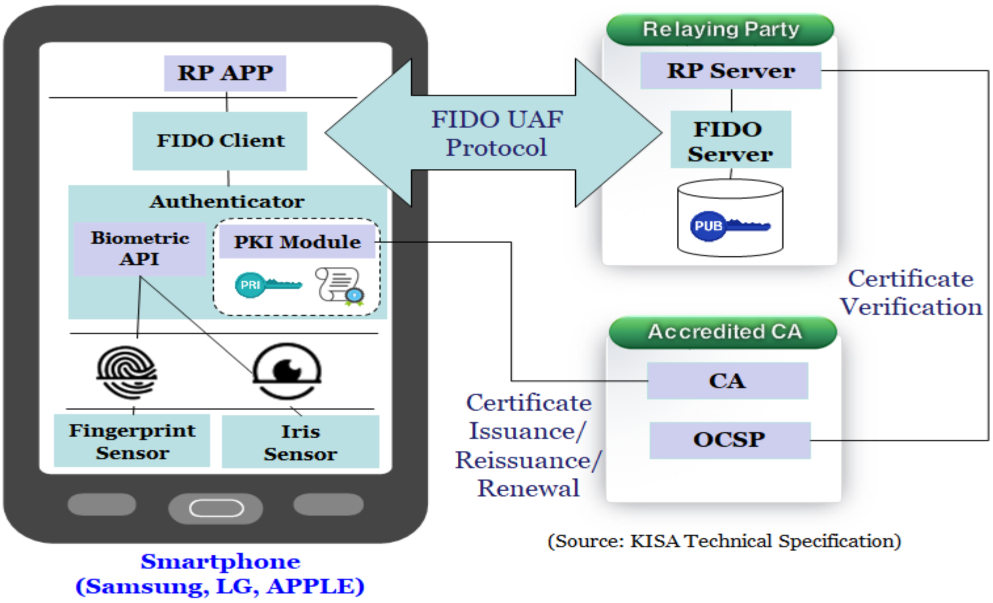
K-FIDO stands for biometric accredited certification service that provides accredited certificate without password using FIDO. K-FIDO uses biometric authentication such as fingerprint in smartphones instead of passwords. K-FIDO specification will be published by KISA (Korea Internet Security Agency).



(Source: Wooribank App with Samsung Pass)

Figure 11. The Basic Concept of K-FIDO Service.

The K-FIDO service is developed using the extension that is defined by the FIDO UAF Protocol. A service APP will be distributed along with a FIDO Client and a K-FIDO Authenticator in APP stores if the K-FIDO APP is distributed as a software package. The KISA specification [2] recommends using KeyStore, TrustZone, or KeyChain as the storage of accredited certificate and private key. Any types of biometric authentication method such as face, voice, iris, and so on can be added.



(Source: KISA Technical Specification)

Figure 12. The Basic Architecture of K-FIDO Service.

3.3. Service Architecture

The K-FIDO service provides the centralized biometric authentication framework in a Fintech environment where a variety of services need a strong and governmentally endorsed identity binding while protecting user's privacy and increasing convenience of customers.

The K-FIDO service consists of a user, a smartphone, a service provider, a FIDO service provider, and an accredited CA. The user's smartphone contains an RP app, a FIDO client, and one or more authenticators. The user performs bio-authentication by biometric sensors in the user's smartphone such as fingerprint, iris and so on. The service provider offers various applications such as financial service, e.g., Internet banking, easy payment, cyber trading, Internet insurance, etc. The FIDO service provider sets up a FIDO server in his data center and usually contracts with service providers by transaction based payment. The accredited CA issues an accredited certificate for the user after checking the user's identity by the user's certificates issued by the government such as NID card, passport, driver's license, etc.

The K-FIDO service provides additional benefits to the usual FIDO service as follows;

① Service providers don’t need to invest a lot in the early stage for FIDO systems.

② It is possible to ensure reliable services because the FIDO service provider as a trusted third party offers the centralized FIDO authentication.

③ The user’s biometric information is stored in the user’s authenticator bound to his smart phone using FIDO UAF specification and it is more secure than being stored on a server (This is one of the benefits that FIDO UAF provides).

④ It can verify the user’s identity proven by a certification authority which is an identification authority. And it can provide more user-friendly authentication methods because it enables a user to use biometrics instead of certificate’s password.

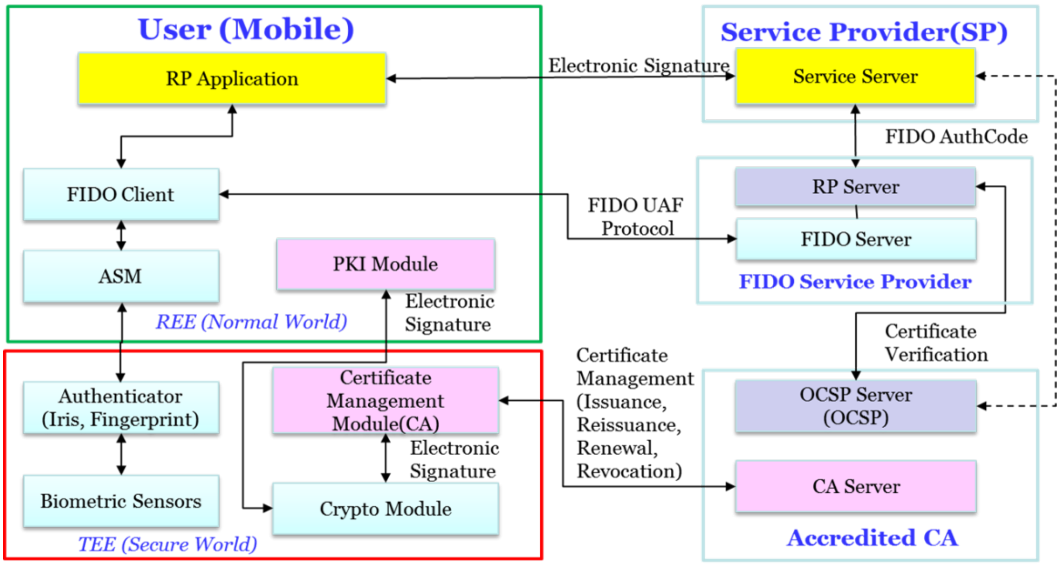


Figure 13. The Architecture of K-FIDO Service.

3.4. Service Process

3.4.1. Registration Process

K-FIDO combines FIDO UAF and PKI. The registration process under the K-FIDO specification is as follows;

① RP App starts bio-registration and requests a user certificate issuance.

② The FIDO server triggers a UAF registration request to the FIDO client.

③ The user performs a bio-authentication with FIDO authenticators using their respective user verification method, e.g. fingerprint, iris, etc.

④ The selected FIDO authenticator generates the FIDO authentication private key. The selected FIDO authenticator generates a FIDO signature using the attestation private key.

⑤ The FIDO server verifies the signature using the attestation public and verifies the authentication public key. If verified, the FIDO server trusts the authenticator it is talking to and the authentication public key that was sent from the authenticator in the authentication response. The FIDO server checks FIDO registration message and if passed, the FIDO server stores the authentication public key.

⑥ The FIDO client requests the user certificate issuance to the certificate management module.

⑦ The crypto module generates a private and public key pair for the user certificate.

⑧ The certificate management module requests the user certificate issuance from the certification authority.

⑨ The certificate management module stores the user certificate and the private key in the secure element such as USIM, Trustzone, etc. However, the private key should be encrypted by an encryption key in keystore or keychain. The registration process is completed.

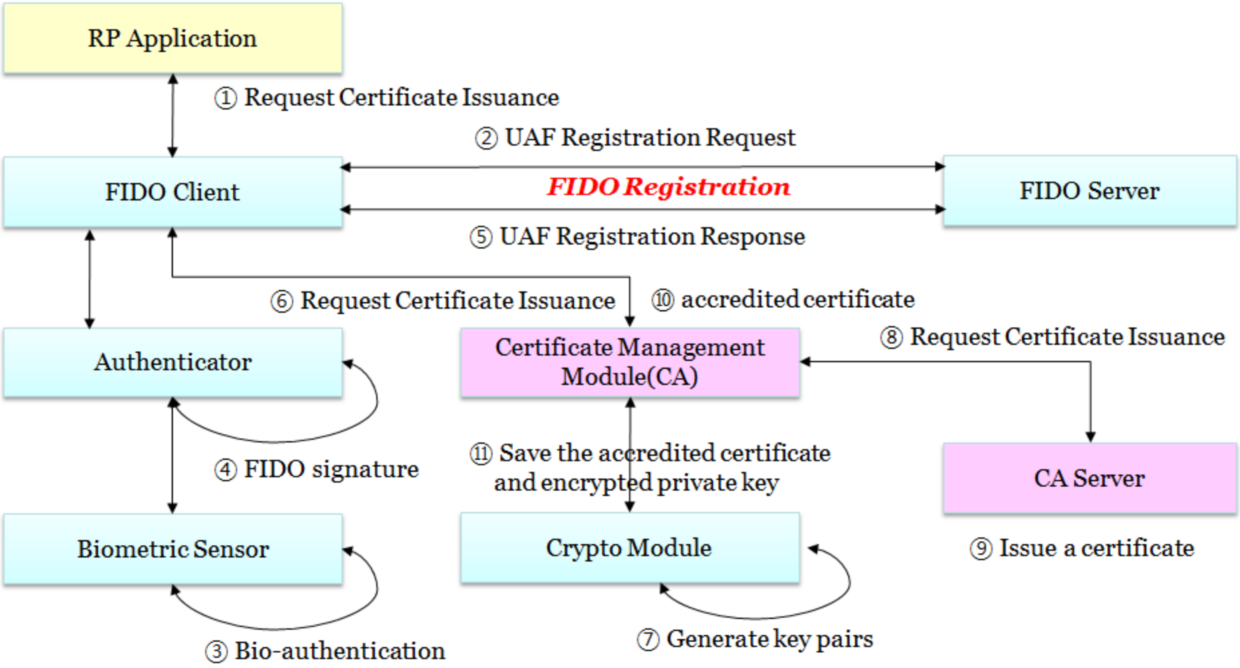

RP Application
① Request Certificate Issuance
② UAF Registration Request
FIDO Client
FIDO Registration
FIDO Server
⑤ UAF Registration Response
⑥ Request Certificate Issuance
⑩ accredited certificate
⑧ Request Certificate Issuance
Authenticator
Certificate Management Module(CA)
④ FIDO signature
⑪ Save the accredited certificate and encrypted private key
CA Server
Biometric Sensor
Crypto Module
⑨ Issue a certificate
③ Bio-authentication
⑦ Generate key pairs

Figure 14. Registration process of K-FIDO Service.

Notes on user's identity:

- Before step six happens where the FIDO client requests the user certificate issuance, the user is assumed to have finished user identification using such a mechanism like mobile authentication, accredited certificate, bank account authentication, etc. A mobile authentication case is shown in the Wooribank use case below. Thus, the user identity is known at the sixth step.

- The user uses FIDO authentication after the user has finished identification, while it is not tightly coupled. The general scenarios are as follows;

  1) A user performs user's identification defined by a service provider.

  2) A user uses FIDO or K-FIDO service (the scope of K-FIDO).

- Authenticators decide where the user certificates are stored. KISA recommends secure elements such as keyStore, keyChain, USIM, or Trustzone, etc.

3.4.2. Authentication Process

With various user service environments, the authentication process that uses a biometric and a certificate in a smartphone is as follows:

① RP App performs bio-authentication and requests electronic signature for a service provider.

② FIDO server triggers UAF authentication request to FIDO client.

③ A User performs a bio-authentication by the FIDO authenticator using the same method as at Registration time.

④ The FIDO authenticator generates FIDO signature (using the FIDO authentication private key).

⑤ The FIDO client sends UAF authentication response to FIDO server. The FIDO server checks FIDO authentication message and if passed, the RP server generates an Authcode.

⑥ The FIDO client requests electronic signature generation to PKI module.

⑦ The PKI module requests electronic signature generation to Crypto module.

⑧ In case of secure element such as Trustzone, or USIM, the electronic signature will be generated by the private key inside the secure element. However, in case of keystore or keychain, the encrypted private key should be decrypted by a decryption key stored in keystore or keychain and electronic signature will be generated by the private key with crypto module.

⑨ PR App sends the signed data to Service server.

⑩ Service server verifies the signed data.

⑪ Service server or RP Server checks user certificate’s verification from OCSP server.

⑫ Service server checks the Authcode from FIDO service provider. And Service server sends the result to the user.

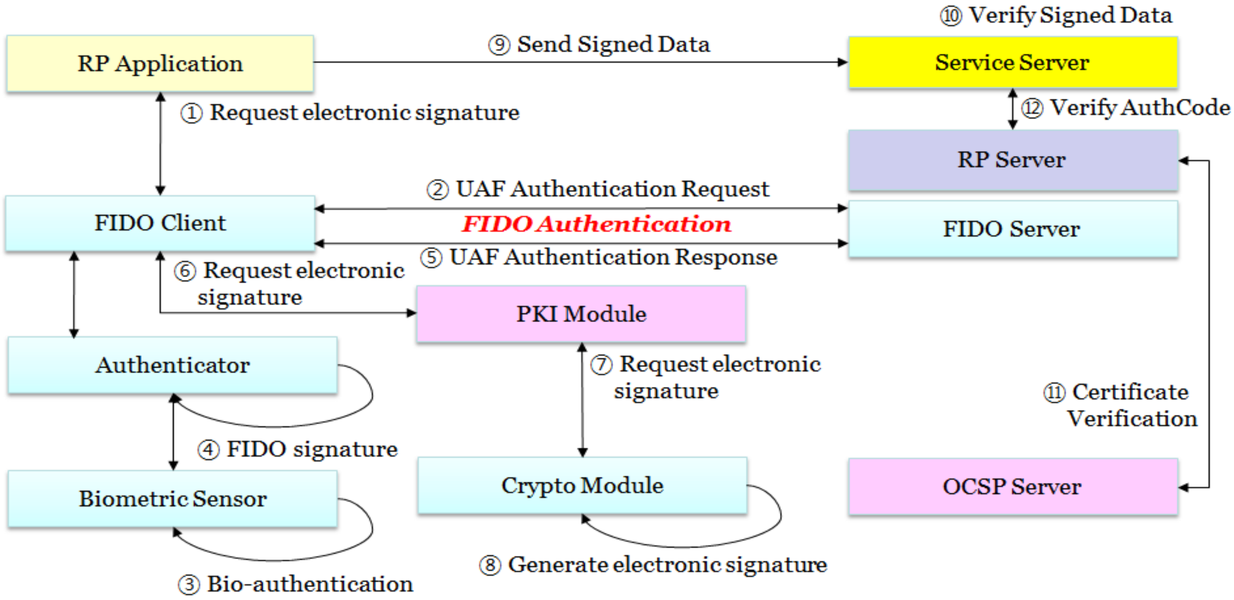


Figure 15. Authentication Process of K-FIDO Service.

3.5. Sequence Diagram

3.5.1. Registration Process

The registration of K-FIDO service added some functions to the FIDO registration protocol as follows;

① RP app requests a certificate issuance from the FIDO client.

② The FIDO client requests a certificate issuance from the authenticator (using the FIDO UAF Extensions).

③ The authenticator generates two sets of key pairs, one for FIDO authentication and the other for a user certificate, and issues a user certificate from a certification authority. The key pair for FIDO authentication is different from the key pair for certificate because of separation of key usage.

④ The authenticator creates a digital signature by the authenticator's attestation private key and sends it to the FIDO server (FIDO UAF Registration response).

⑤ The FIDO server verifies the signed data using the attestation public key of the authenticator and, if correct, saves the user's public key, the user certificate, and the authentication public key of the user in the server.

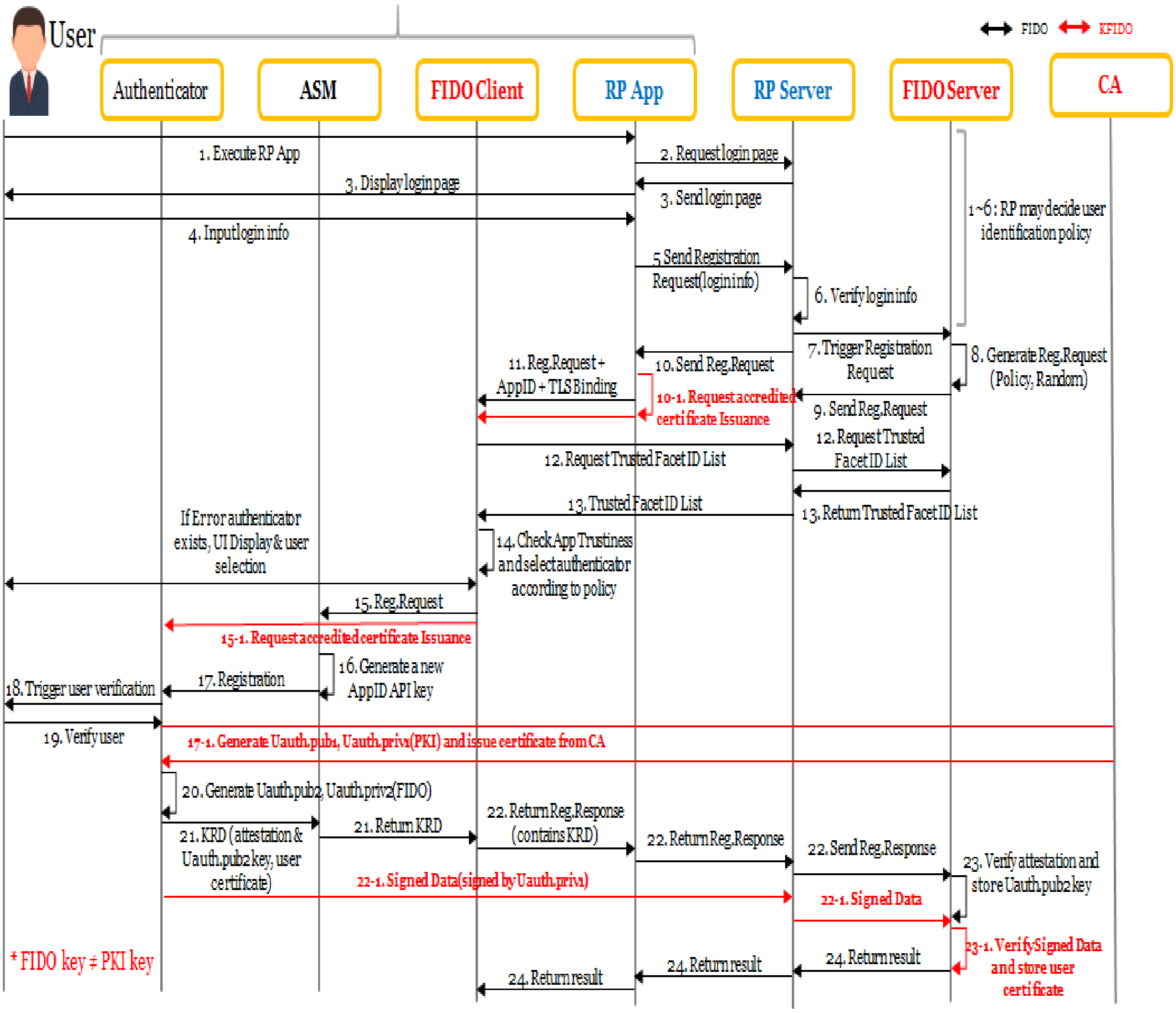

User
FIDO
KFIDO
Authenticator
ASM
FIDO Client
RP App
RP Server
FIDO Server
CA
1. Execute RP App
2. Request login page
3. Display login page
3. Send login page
1~6 : RP may decide user identification policy
4. Input login info
5 Send Registration Request(login info)
6. Verify login info
7. Trigger Registration Request
8. Generate Reg.Request (Policy, Random)
11. Reg.Request + AppID + TLS Binding
10. Send Reg.Request
10-1. Request accredited certificate Issuance
9. Send Reg.Request
12. Request Trusted FacetID List
12. Request Trusted FacetID List
13. Trusted FacetID List
13. Return Trusted FacetID List
If Error authenticator exists, UI Display & user selection
14. Check App Trustiness and select authenticator according to policy
15. Reg.Request
15-1. Request accredited certificate Issuance
16. Generate a new AppID API key
18. Trigger user verification
17. Registration
19. Verify user
17-1. Generate Uauth.pub1, Uauth.priv1(PKI) and issue certificate from CA
20. Generate Uauth.pub2, Uauth.priv2(FIDO)
21. KRD (attestation & Uauth.pub2 key, user certificate)
21. Return KRD
22. Return Reg.Response (contains KRD)
22. Return Reg.Response
22. Send Reg.Response
23. Verify attestation and store Uauth.pub2 key
22-1. Signed Data(signed by Uauth.priv1)
22-1. Signed Data
23-1. Verify Signed Data and store user certificate
* FIDO key ≠ PKI key
24. Return result
24. Return result
24. Return result

Figure 16. Registration Flow Chart.

3.5.2. Authentication Process

The authentication of K-FIDO service added some functions to the FIDO UAF authentication protocol as follows;

① The RP app sends the certificate of the service providers to FIDO client. The purpose of the server certificate is to enable FIDO client to check the server identity and to encrypt sensitive data that are sent to the service server.

② The authenticator generates a digital signature using the private key that was generated by the PKI module in the registration process. The signed data is sent to the RP server in the authentication response using the UAF message Extension. Third, RP server verifies the status of user's certificate from OCSP (Online Certificate Status Protocol) server and verifies the signed data. The Online Certificate Status Protocol (OCSP) was created as an alternative to certificate revocation lists (CRLs). Similar to CRLs, OCSP enables a requesting party (e.g., a web browser) to determine the revocation state of a certificate.

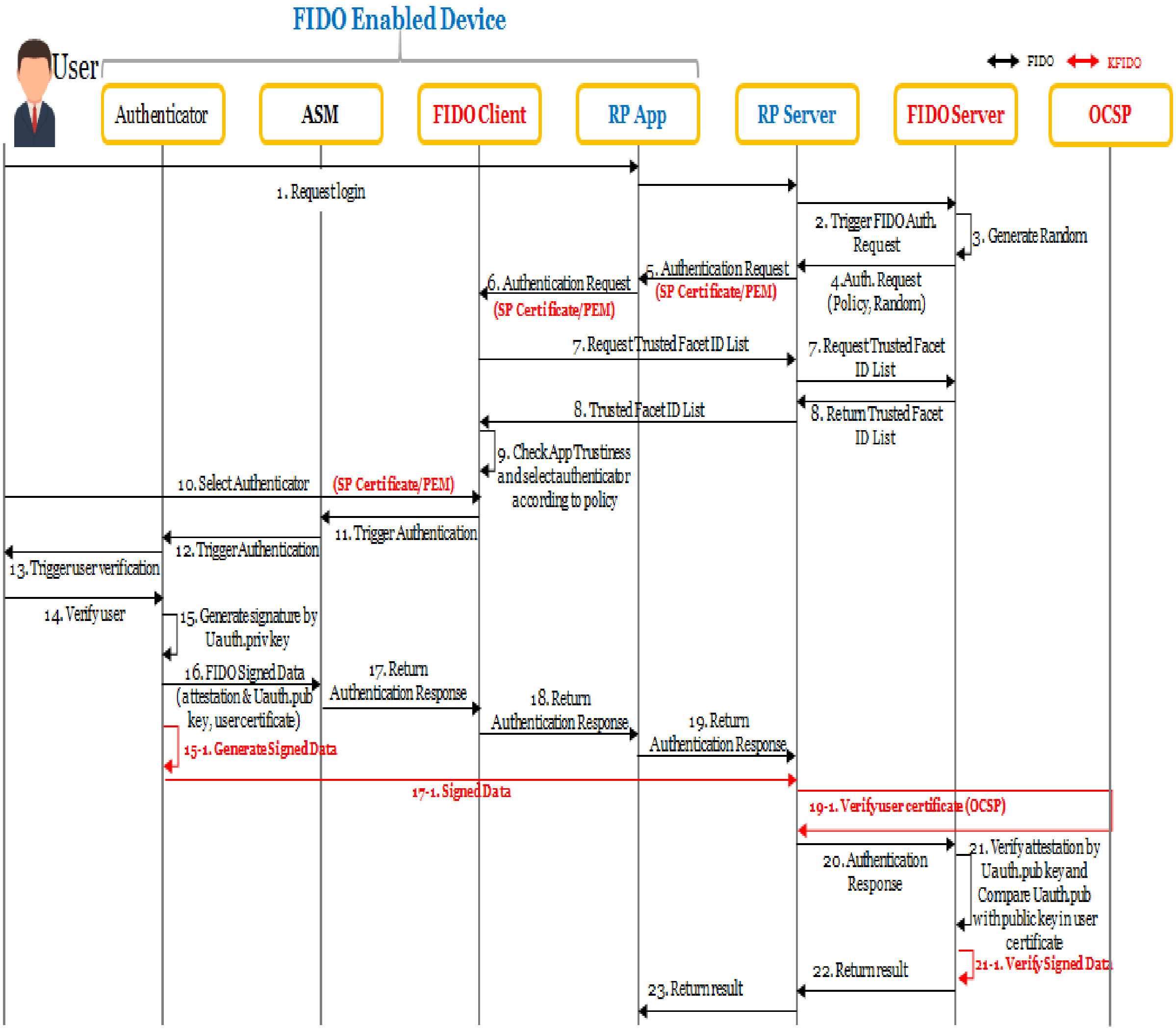
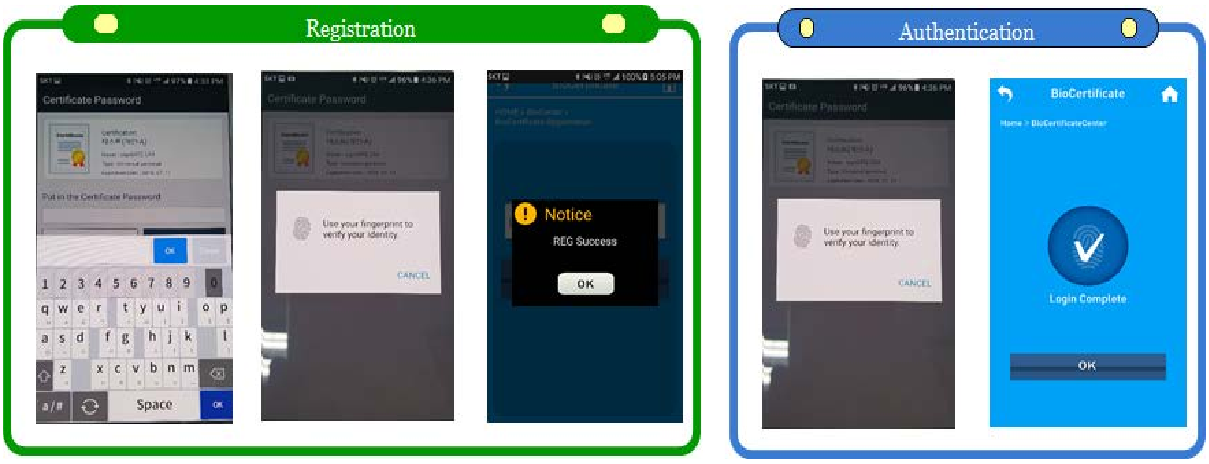

FIDO Enabled Device
User
FIDO
KFIDO
Authenticator
ASM
FIDO Client
RP App
RP Server
FIDO Server
OCSP
1. Request login
2. Trigger FIDO Auth. Request
3. Generate Random
4.Auth. Request (Policy, Random)
5. Authentication Request (SP Certificate/PEM)
6. Authentication Request (SP Certificate/PEM)
7. Request Trusted Facet ID List
7. Request Trusted Facet ID List
8. Trusted Facet ID List
8. Return Trusted Facet ID List
9. Check App Trustiness and select authenticator according to policy
10. Select Authenticator
(SP Certificate/PEM)
11. Trigger Authentication
12. Trigger Authentication
13. Trigger user verification
14. Verify user
15. Generate signature by Uauth.priv key
16. FIDO Signed Data (attestation & Uauth.pub key, user certificate)
15-1. Generate Signed Data
17. Return Authentication Response
17-1. Signed Data
18. Return Authentication Response
19. Return Authentication Response
19-1. Verify user certificate (OCSP)
20. Authentication Response
21. Verify attestation by Uauth.pub key and Compare Uauth.pub with public key in user certificate
21-1. Verify Signed Data
22. Return result
23. Return result

Figure 17. Authentication Flow Chart.

3.6. K-FIDO DEMO APP

3.6.1. Overview

The K-FIDO system based on Android 6.0 in Samsung Galaxy S7 having a fingerprint sensor was developed by KICA [3]. This system has two main functions; one is registration, and the other is authentication. The registration process has three steps. First, a user enters the password for the selected accredited certificate. Second, if matched, it perform fingerprint authentication Third, if succeeded, the user completes fingerprint registration for the accredited certificate. The authentication process is that a user selects an accredited certificate to use and authenticated with a registered fingerprint, and if matched, login process will be succeeded.



Put in the Certificate Password

Use your fingerprint to verify your identity.

REG Success

Use your fingerprint to verify your identity.

Login Complete

Figure 18. User Interface Example of Registration and Authentication.

3.6.2. Service Flow

The implemented authentication process with user's device, Service Provider, and FIDO Service Provider is as follows;

① User wants to use a special service with biometric authentication in User's device. An RP App starts bio-authentication.

② The RP App requests FIDO based authentication to a mobile manufacturer's FIDO client or a security company's FIDO client.

③ The FIDO Client calls authenticators.

④ The User performs bio-authentication by a FIDO authenticator such as fingerprint, iris, etc.

⑤ The FIDO client sends a FIDO authentication message to a FIDO server using the FIDO UAF authentication protocol.

⑥ The FIDO server checks the FIDO authentication message and if passed, the RP server generates an Authcode.

⑦ The RP server sends the authentication result and the Authcode to the User.

⑧ The RP app sends the Authcode to the Service Provider.

⑨ The Service Provider requests the Authcode verification to a Front-end Processor (FEP) server in a FIDO Service Provider.

⑩ The FEP server compares the received Authcode with the stored Authcode, and if matched, sends the success result.

⑪ The Service Provider returns the result to the User.

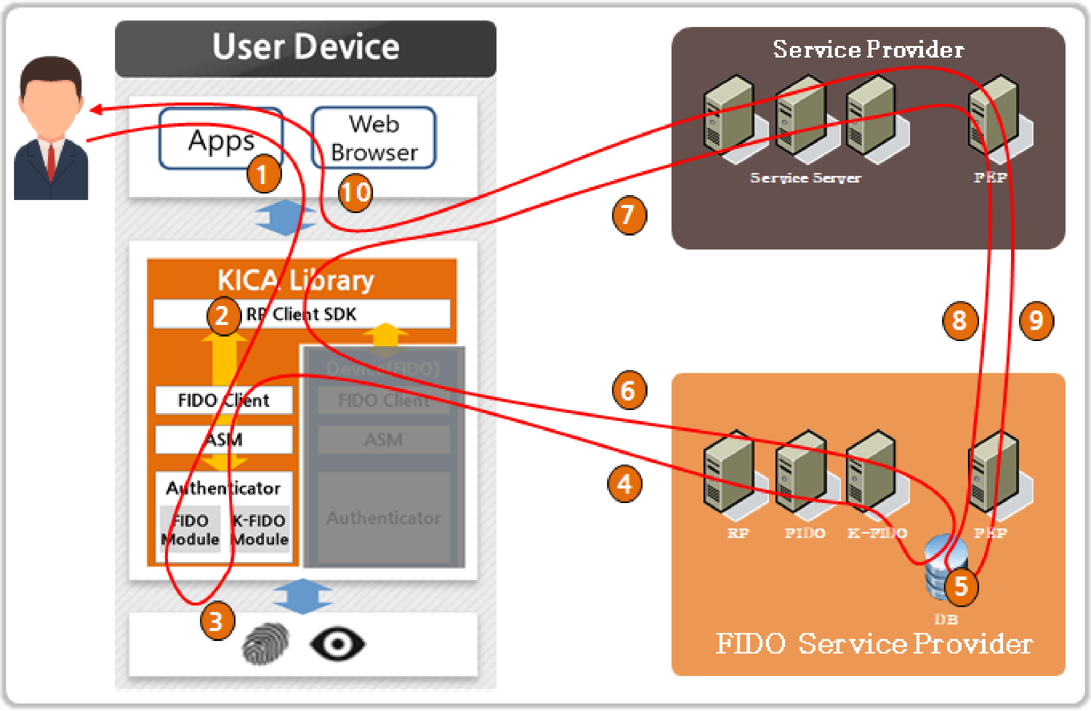


Figure 19. Authentication Process of K-FIDO Demo.

3.7. Comparison with FIDO and K-FIDO

FIDO UAF protocol only checks the owner of the authenticator but K-FIDO checks the user's identity by an accredited certificate issued by face-to-face identification through one of National ID Card, driver license card, passport, etc. FIDO uses the same origin policy based on each sites. The FIDO client triggers the generation of different FIDO authentication key pairs for different sites. But K-FIDO uses one key pair and one certificate for all sites/applications in order to tie the authentication to a single Governmentally endorsed identity. The old version of FIDO authenticators didn't support the FIDO server to distinguish different fingers, but the new version of FIDO specification supports User Verification Index (UVI) that is a value uniquely identifying a user verification data record. K-FIDO supports both single matching policy and multiple matching policy. The most of service providers select single match policy that uses the same fingerprint as the registered fingerprint during registration process. The biometric authentication of single matching policy is more secure than that of multiple matching policy (The financial sectors in Korea are required to use single matching policy. So K-FIDO has followed by the policy).

FIDO supports biometric user verification but K-FIDO combines FIDO and PKI technology. FIDO and K-FIDO use the same FIDO UAF protocol. K-FIDO adds electronic signature function using the extension of FIDO protocol.

Table 2. The Comparison of FIDO and K-FIDO.

Category	FIDO	K-FIDO
Identification	Out of scope for FIDO – depends on identity binding.	Verify user's Identity backed by some Government ID
Authentication event always tied to single identity	No. One authentication key per account in order to avoid global correlation handles.	Yes (certificate)
Biometric information	Multiple matching policy. Single matching policy supported by some authenticators (called UVI).	Single matching policy, Multiple matching policy.
Service area	Password alternatives	Certificate Password alternatives
User verification method	Biometric, PIN pattern based, etc.	Biometric, PIN pattern based, etc.
Authentication protocol	FIDO, based on public key cryptography	TLS client certificates, based on PKI or FIDO.
International standard	FIDO UAF protocol	FIDO UAF protocol(+ X.509)

4. Case Study of K-FIDO business in Korea

4.1. Bank Area: Wooribank[4]

This model provides an iris authentication of Samsung Pass instead of accredited certificate password for site login, money transfer and so on using Samsung smartphones.

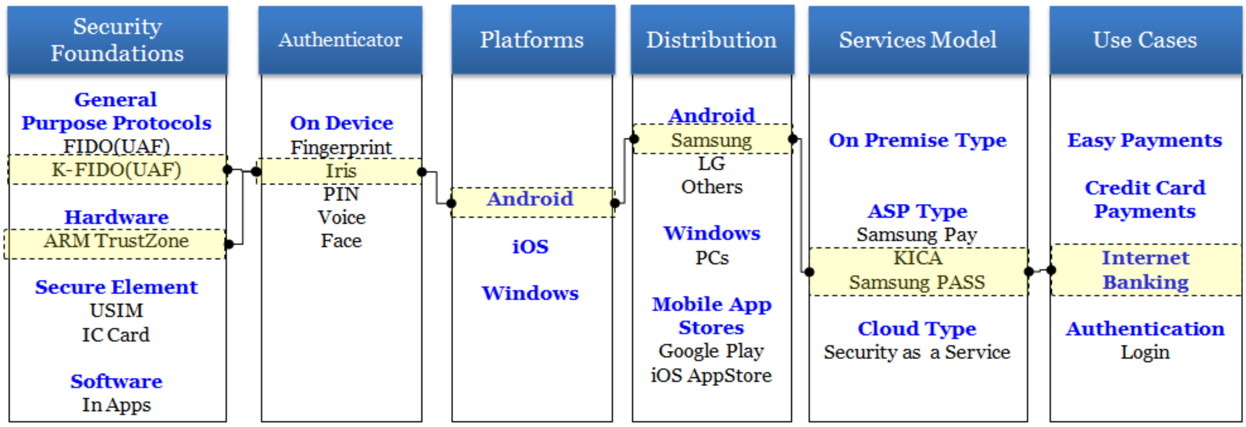


Figure 20. Implementation Choices of Wooribank Case.

4.1.1. Registration Process

A user has to register Wooribank APP in order to use iris based authentication as follows;

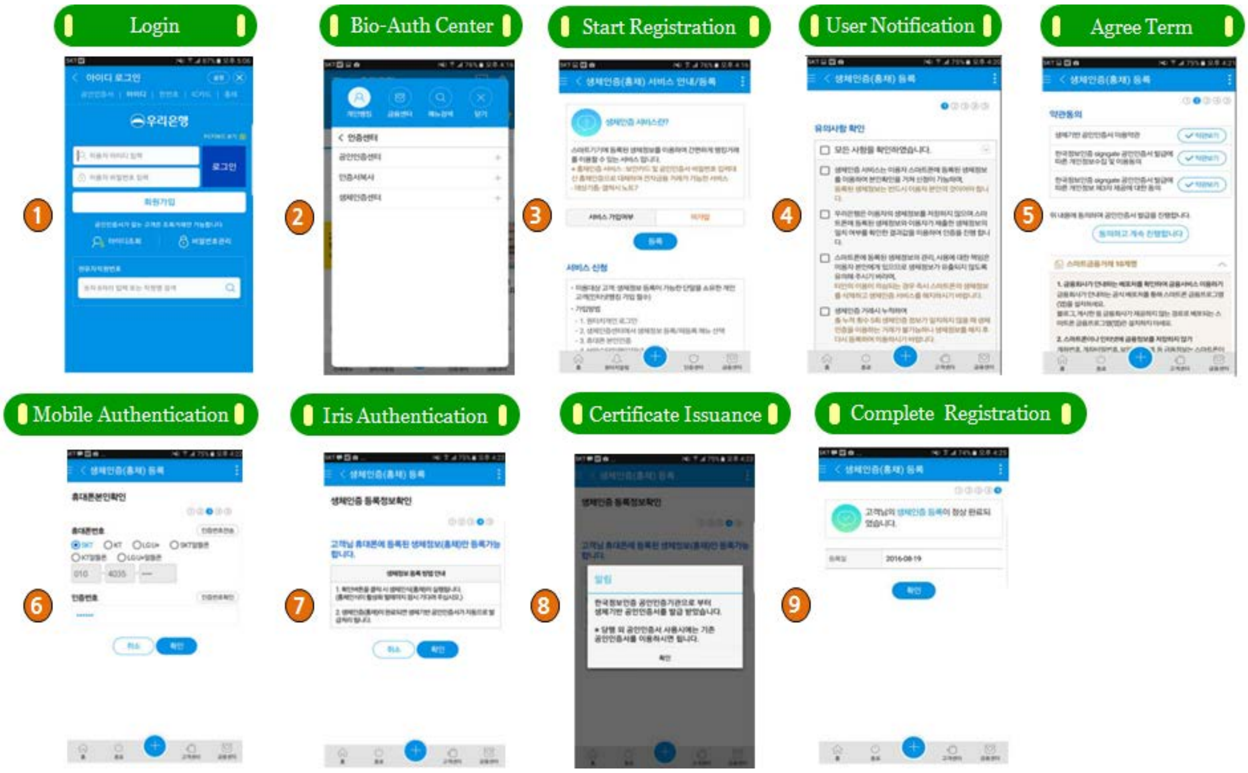


Figure 21. Registration using iris based authentication.

① The user reads user notification and agrees to the term and conditions of the service.

② The user performs mobile authentication with her/his mobile information.

③ If passed, the user checks iris authentication.

④ If the verification is succeeded, the user issues accredited certificate from certification authority.

⑤ The registration is finished if the certificate is stored in a secure area in smart phones.

4.1.2. Login Process and Money Transfer Process

The user can login the Wooribank APP with iris authentication.

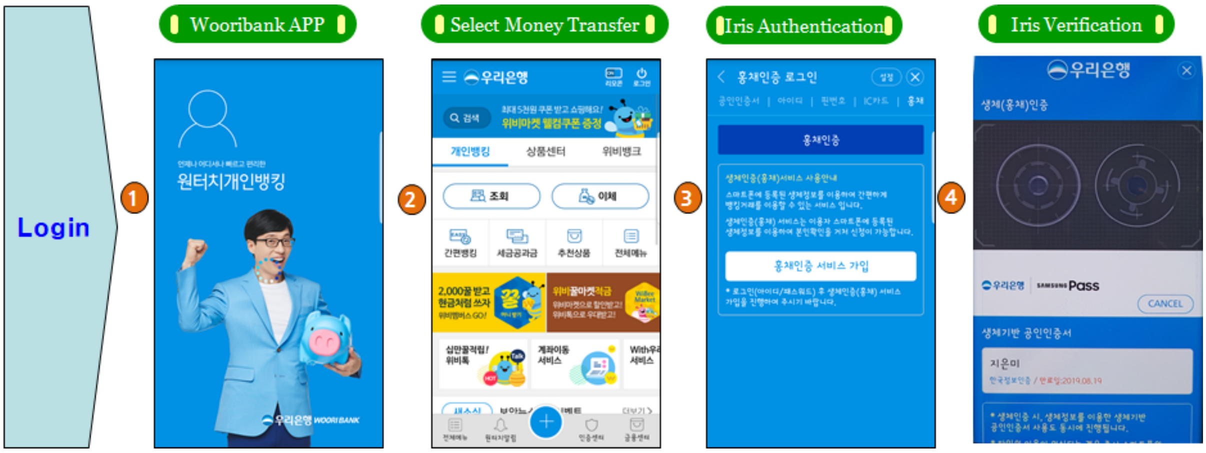


Figure 22. Login with iris authentication.

The user can transfer money with iris authentication.

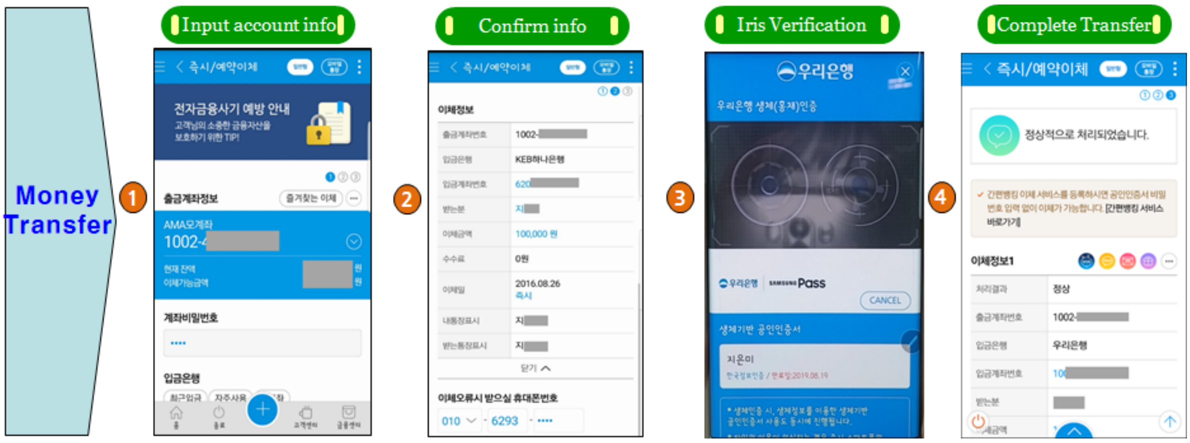


Figure 23. Money transfer with iris authentication.

5. Conclusion

In this white paper, we have introduced how K-FIDO service combines FIDO and PKI in a smartphone for a successful nationwide FIDO deployment in Korea. This framework can be a solution to the problems due to lack of user's identification and limitation of the current FIDO service. By incorporating PKI's identification and FIDO's biometric authentication, this system will benefit everyone who wants to have a safe and convenient smartphone authentication environment.

6. Acknowledgements

The author gratefully acknowledges the valuable advises from Dr. Max Hata, the Co-Chair of Deployment at Scale WG of FIDO Alliance and Dr. Rolf Lindemann from NokNok Labs.

7. References

[1] FIDO UAF Architectural Overview (FIDO Alliance, December 2014)

https://fidoalliance.org/specifications/download/

[2] Implementation Guideline for Safe Usage of Accredited Certificate using bio information in Smart phone (KISA, September 2016)

http://rootca.kisa.or.kr/kcac/down/Guide/Implementation%20Guideline%20for%20Safe%20Usage%20of%20Accredited%20Certificate%20using%20bio%20information%20in%20Smart%20phone.pdf (Korean)

[3] KICA (Korea Information Certificate Authority)

(English) https://www.kica.co.kr/kica/eng/main/formMain.sg

(Korean) http://www.signgate.com

[4] Woori Bank

(Korean) http://www.wooribank.com

[5] FIDO Privacy, FIDO Alliance White Paper, 19 January 2016, https://fidoalliance.org/resources/FIDO__Privacy_White_Paper_Jan_2016.pdf