International Journal of Security and Its Applications
Vol. 10, No. 12 (2016), pp.69-80
http://dx.doi.org/10.14257/ijsia.2016.10.12.07

Design of a Secure Biometric Authentication Framework Using PKI and FIDO in Fintech Environments

Jae Jung Kim[1] and Seng Phil Hong[2]

Department of Computer Science, Sungshin Women's University, Seoul, Korea
[1]jajukim@gmail.com, [2]philhong@sungshin.ac.kr

Abstract

It goes without saying that the use of FIDO based services, especially financial areas is becoming more and more widespread these days. FIDO services are adapting a variety of service areas such as easy payment, money transfer, ATM withdrawal/savings, and single sign-on, etc. Because FIDO service uses standard public key cryptography techniques to provide stronger authentication and securely saves a user's bio-information in the smartphone. But when registered, FIDO only confirms the match between pre–enrolled fingerprints and the one on the registration process. In other words, FIDO is not able to verify the person's identity. The user has to register his/her biometric information in each sites. It is our purpose to solve these problems by implementing FIDO and PKI technologies adapted in current FIDO service and accredited certification system. The proposed secure biometric authentication framework provides the centralized biometric authentication framework in Fintech environment that a variety of services need the interoperability of user's biometric information in order to protect user's privacy and increase convenience of customers.

Keywords: *Biometric Authentication, FIDO(Fast Identity Online), PKI(Public Key Infrastructure)*

1. Introduction

Fintech is a service sector which uses mobile-centered IT technology to enhance the efficiency of the financial system. [1] Fintech encompasses all technical processes related with financial services including mobile payment and remittance, private asset management and crowdfunding [2] As biometric authentication methods become more and more common in daily life we have seen an increased interest and developments of more convenient and secure authentication methods for online services. With biometrics enabled smartphones the cost associated with deploying biometric systems is removed and the opportunity for use in new applications is opened. [3]

FIDO Alliance is nominally formed in July 2012. The board level members are global companies such as Google, Microsoft, Samsung, PayPal, MasterCard, VISA, RSA, etc. The FIDO Alliance plans to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms that supplant reliance on passwords to securely authenticate users of online services. The FIDO protocols use standard public key cryptography techniques to provide stronger authentication. The FIDO protocols consist of registration, authentication, transaction confirmation, and deregistration. The registration Process is as follows; First, User is prompted to choose an available FIDO authenticator that matches the online service's acceptance policy. Second, User unlocks the FIDO authenticator using a fingerprint reader, a button on a second–factor device, securely–entered PIN or other method. Third, User's device creates a new public/private key pair unique for the local device, online service and user's account. Fourth, Public key is sent to the online service and associated with the user's account. The private key and any information about the local

ISSN: 1738-9976 IJSIA

authentication method (such as biometric measurements or templates) never leave the local device.

The authentication process is as follows; First, Online service challenges the user to authenticate with a previously registered device that matches the service's acceptance policy. Second, User unlocks the FIDO authenticator using the same method as at Registration time. Third, Device uses the user's account identifier provided by the service to select the correct key and sign the service's challenge. Fourth, Client device sends the signed challenge back to the service, which verifies it with the stored public key and authenticates the user [4, 5].

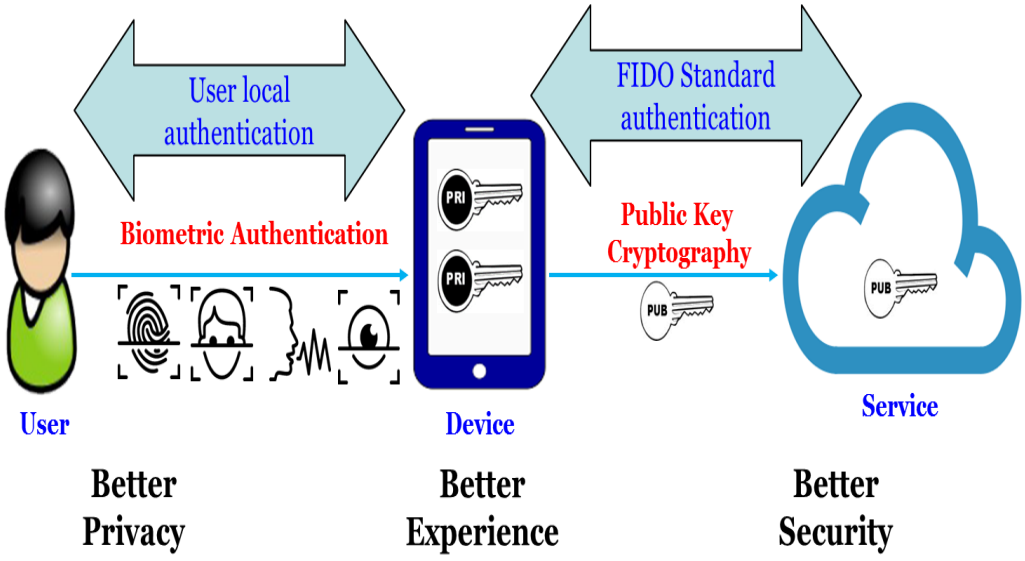

Figure 1. FIDO UAF Architecture

Digital certificates are one of the many solutions available for authentication, but they are easy to copy and leak. Mobile device services need to properly manage registered devices and users, and trusted means of authenticating their identities are needed. [6] 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 [7].

2. Problem Statement

We analyzed the status and problems of the current FIDO based bio-authentication system and have suggestions for improvement.

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

The current biometric authentication framework is that service providers use FIDO [8] solutions for their services. So a user has to register his/her biometric information each sites in order to use each services. It doesn't provide the interoperability among each services.

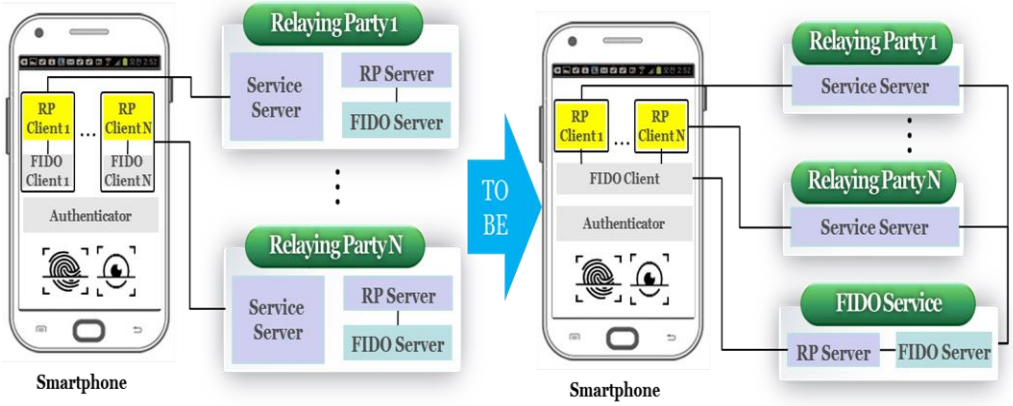

Figure 2. The Current Biometric Authentication Framework

2.2. The Verification of Person's Identity in FIDO

The process of authentication and registration of FIDO is preceded under the control of smartphone user. In the case of a fingerprint sensing authenticator, the user must register their fingerprint(s) with the authenticator. Once enrollment is complete, the FIDO UAF authenticator is ready for registration with FIDO UAF enabled online services and websites.

When registered, FIDO only confirms the match between pre–enrolled fingerprint and the one on the process. In other words, FIDO is not able to 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 [9].

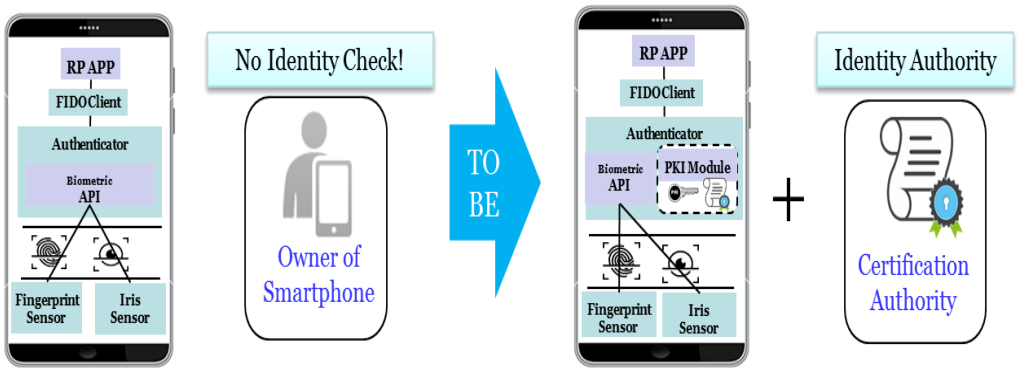

Figure 3. Comparison of Identification Methods

3. The Secure Biometric Authentication Framework using PKI and FIDO

The SBAF provides the centralized biometric authentication framework in Fintech environment that a variety of services need the interoperability of user's biometric information in order to protect user's privacy and increase convenience of customers.

3.1. Architecture of Secure Biometric Authentication Framework (SBAF)

The secure biometric authentication framework consists of a user, a smartphone, service provider, FIDO service provider, and accredited CA. A user's smartphone

contains RP app, FIDO client, and authenticator. A user performs bio-authentication by biometric sensor in user's smartphone such as fingerprint, iris and so on. Service provider offers a lot of applications such as financial service such as internet banking, easy payment, cyber trading, internet insurance, *etc*. FIDO service provider sets up a FIDO server in his data center and usually contracts with service provider by transaction based payment. An accredited CA issues an accredited certificate for users after checks user's identity by certificates issued by government such as NID card, passport, driver's license, *etc.*

The SBAF provides a lot of benefits compared to traditional FIDO service as follows; First, service providers don't need to invest a lot in the early stage for FIDO system. Second, it is possible to ensure reliable service because the FIDO service provider as a trust third parity offers the centralized FIDO authentication. Third, the user's biometric information is stored in user's smart phone using FIDO UAF specification and it is more secure than stored on a server. Fourth, it can verify user's identification from certification authority as identify authority. And we can provide more user-friendly authentication methods because a user use biometric such as fingerprint or iris instead of certificate password.

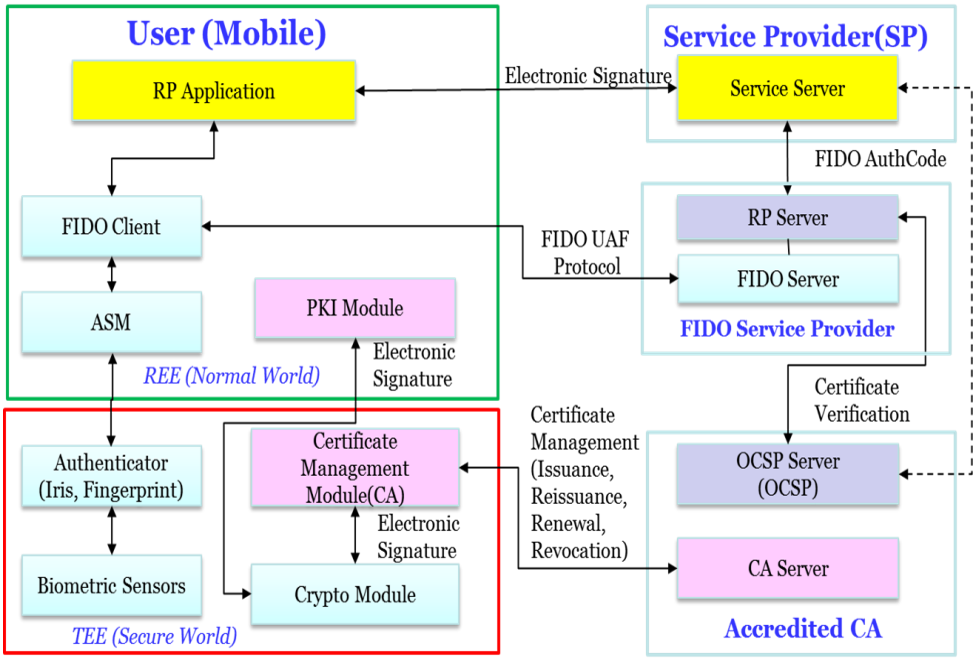

Figure 4. Secure Biometric Authentication Framework

3.2. Registration Process

The registration process that combines with FIDO and PKI in a smartphone is as follows;

First, RP App starts bio-registration and requests certificate issuance for a user. Second, FIDO server triggers UAF registration request to FIDO client. Third, a user performs a bio-authentication by FIDO authenticators such as fingerprint, iris, etc. Fourth, the selected FIDO authenticator generates FIDO signature. Fifth, the FIDO server checks FIDO registration message and if passed, the FIDO server sends UAF registration response to the FIDO client. Sixth, the FIDO client requests certificate issuance to certificate management module. Seventh, Crypto module generates key pairs for certificate using a secure element. Eighth, the certificate management module requests certificate issuance to certification authority. Ninth, the certificate management module

stores the certificate and the encrypted private key in the secure element, and the registration process is completed.

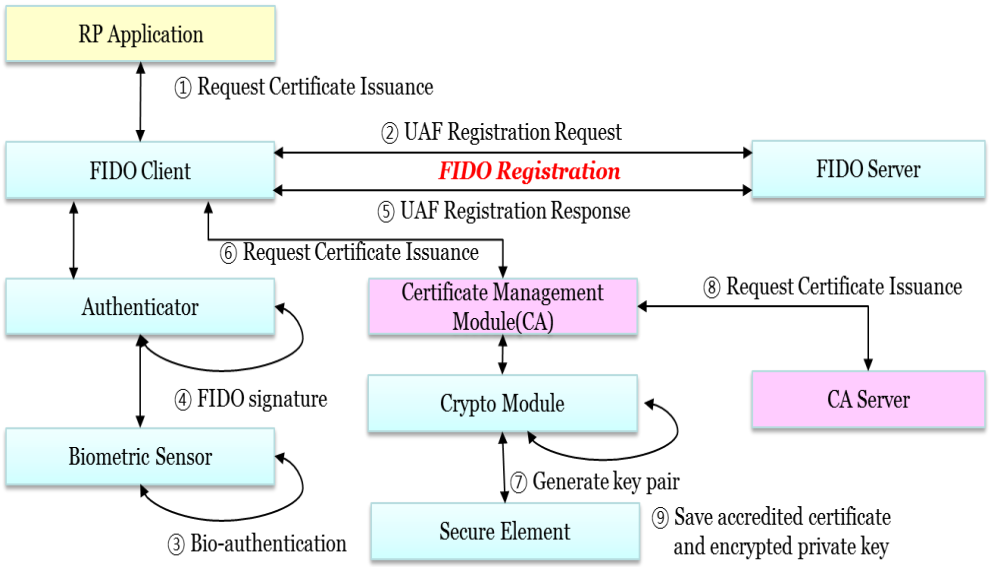

Figure 5. Registration process of SBAF

3.2.1. Flow chart of Registration

The FIDO UAF registration protocol enables Relying Parties to:

- Discover the FIDO UAF Authenticators available on a user's system or device. Discovery will convey FIDO UAF Authenticator attributes to the Relying Party thus enabling policy decisions and enforcement to take place.
- Verify attestation assertions made by the FIDO UAF Authenticators to ensure the authenticator is authentic and trusted. Verification occurs using the attestation public key certificates distributed via authenticator metadata.
- Register the authenticator and associate it with the user's account at the Relying Party. Once an authenticator attestation has been validated, the Relying Party can provide a unique secure identifier that is specific to the Relying Party and the FIDO UAF Authenticator. This identifier can be used in future interactions between the pair {RP, Authenticator} and is not known to any other devices. [8]

The registration of SBAF is added some functions in FIDO registration protocol as follows; First, RP app requests a certificate issuance to FIDO client. Second, the FIDO client requests a certificate issuance to an authenticator. Third, the authenticator generates key pairs and issues a certificate from certification authority. The key pairs of FIDO are different from the key pairs of certificate because of separation of key usage. Fourth, the authenticator signs digital signature by the private key of user and sends it to FIDO server. Fifth, the FIDO server verifies the signed data and if correct, saves the user's certificate.

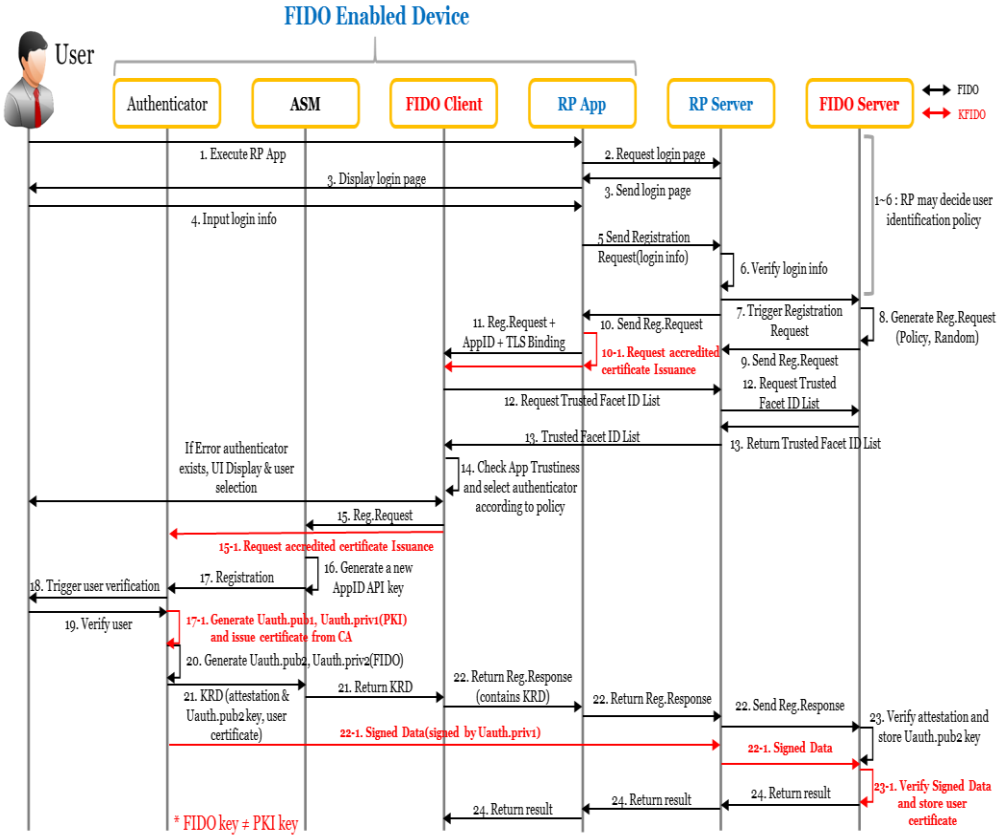

Figure 6. Registration Flow Chart of SBAF

3.3. Authentication Process

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

First, RP App performs bio-authentication and requests electronic signature for a service provider. Second, FIDO server triggers UAF authentication request to FIDO client. Third, a User performs a bio-authentication by the FIDO authenticator using the same method as at Registration time. Fourth, FIDO authenticator generates FIDO signature. Fifth, the FIDO server checks FIDO authentication message and if passed, the RP server generates an Authcode. FIDO server sends UAF authentication response to FIDO client. Sixth, FIDO client requests electronic signature generation to PKI module. Seventh, PKI module requests electronic signature generation to Crypto module. Eighth, the private key stored in secure elements such as Trustzone, USIM and so on generates electronic signature of data to be signed. Ninth, PR App sends the signed data to Service server. Tenth, Service server verifies the signed data. Eleventh, Service server or RP Server checks user certificate's verification from OCSP server. Twelfth, Service server checks the Authcode from FIDO service provider. And Service server sends the result to the user.

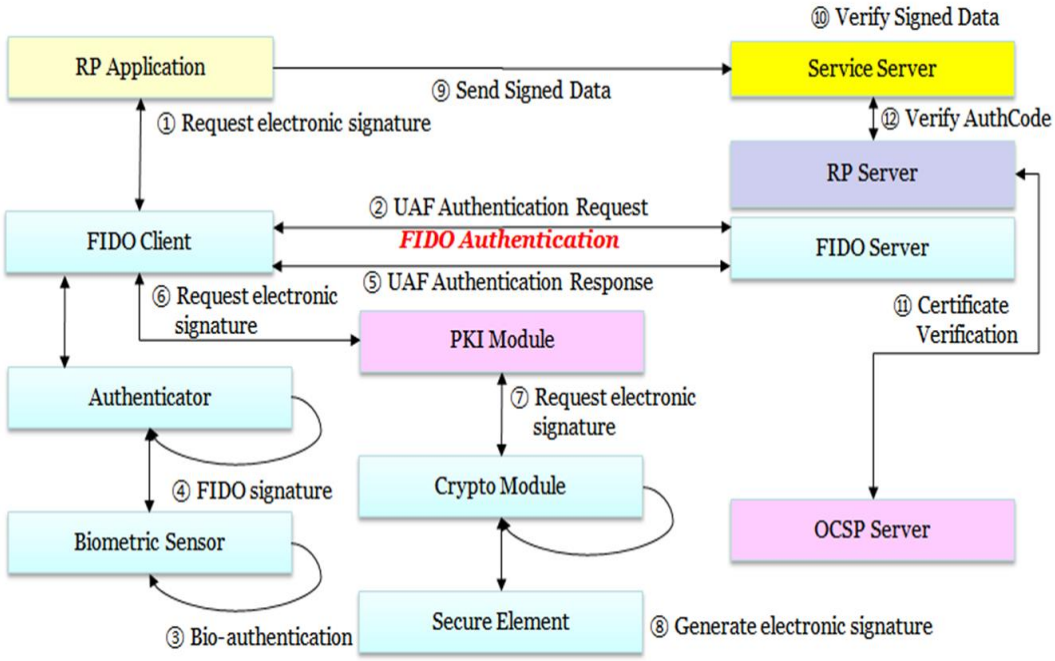

Figure 7. Authentication Process of SBAF

3.3.1. Flow chart of Authentication

The FIDO UAF Authentication protocol is typically based on cryptographic challenge-response authentication protocols and will facilitate user choice regarding which FIDO UAF Authenticators are employed in an authentication event.

Secure Transaction Confirmation: If the user authenticator includes the capability to do so, a Relying Party can present the user with a secure message for confirmation. The message content is determined by the Relying Party and could be used in a variety of contexts such as confirming a financial transaction, a user agreement, or releasing patient records. [8]

The authentication of SBAF is added some functions in FIDO authentication protocol as follows; First, RP app transmits the certificate of service providers. The purpose of server certificate is checked server identity by FIDO client and can be used for encryption of a sensitive data that sends to service server. Second, an authenticator generates digital signature by the private key that registered in registration process. 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. [10]

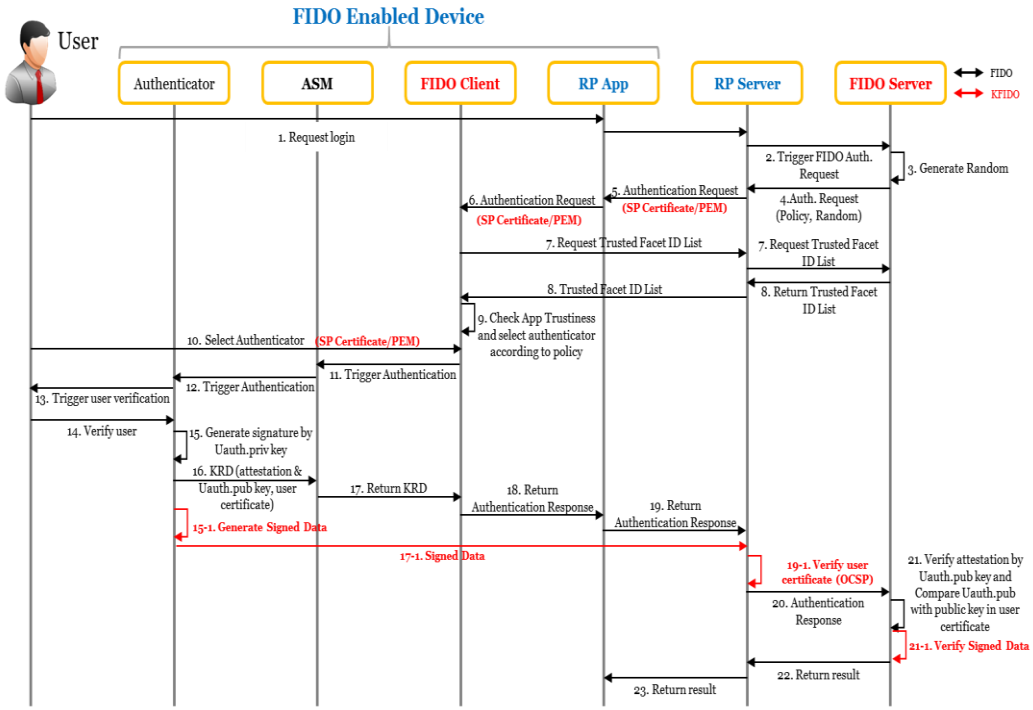

Figure 8. Authentication Flow Chart of SBAF

4. Implementation and Comparison

4.1. Implementation

We developed the SBAF system based on Android 6.0 in Samsung Galaxy S7 having fingerprint sensor.

This system has two main functions, one is registration, and the other is authentication.

The registration process has three steps. First, a user input the password for the selected accredited certificate. Second, if matched, perform fingerprint authentication Third, if succeed, the user completes fingerprint registration for the accredited certificate.

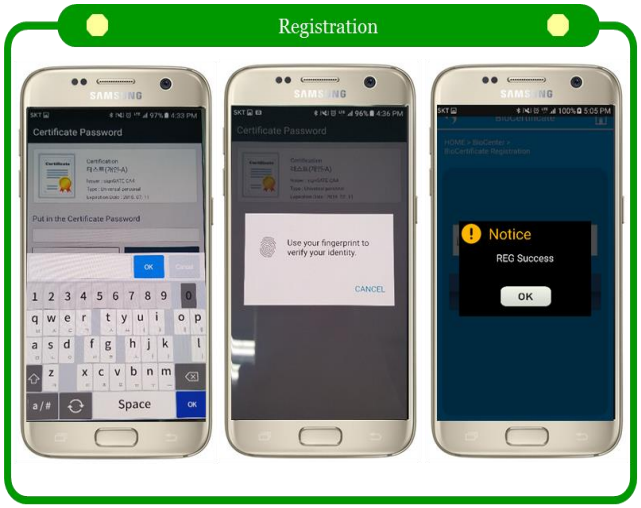

Figure 9. Registration User Interface Example

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 succeed.

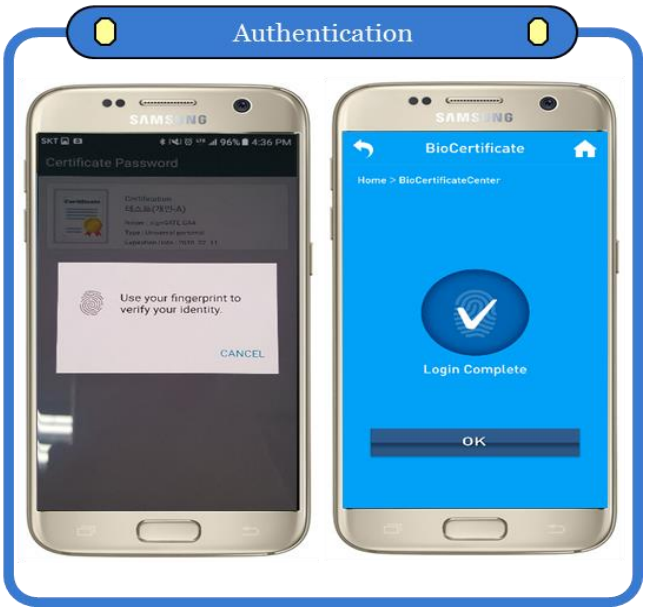

Figure 10. Authentication User Interface Example

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

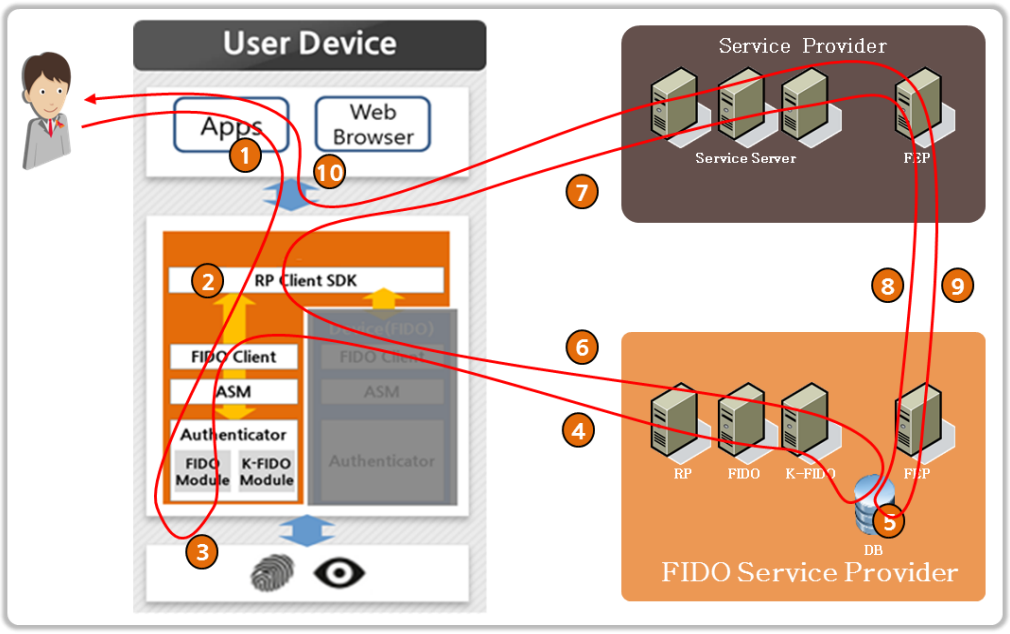

Figure 11. Secure Biometric Authentication Framework

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

② The RP App requests FIDO based authentication to mobile manufacturer's FIDO client or Security Company's FIDO client.

③ The FIDO Client calls authenticators.

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

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

⑥ The FIDO server checks 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 inputted Authcode with the stored Authcode, and if matched, send the success result.

⑪ The Service Provider returns the result to the User.

4.2. Comparison

The proposed system is compared with the current biometric authentication service as follow;

Table 1. Comparison Table

Category	FIDO	SBAF
Identification	Check owner of device	Check User's Identity
Support Interoperability	No (Same origin policy)	Yes (certificate)
Biometric information	Multiple matching policy	Single matching policy
Service area	Password alternatives	Certificate alternatives
Authentication Method	Biometric authentication	Biometric and PKI authentication
International standard	FIDO UAF protocol	FIDO UAF protocol (+ X.509)

FIDO UAF protocol only checks an owner of smartphone but SBAF checks user's identity by an accredited certificate issued by face to face identification. FIDO uses same origin policy based on each sites. FIDO client generates different key pairs for each sites. But SBAF can use one key pairs and certificate for every application in order to provide interoperability among applications. FIDO uses multiple matching policy which only confirms the match between pre–enrolled fingerprints and the one on the registration process. But SBAF have to use the same fingerprint as the registered fingerprint during registration process because of single matching policy. The biometric authentication of single matching policy is more secure than that of multiple matching policy. FIDO only uses biometric authentication but SBAF combines FIDO and PKI technology. FIDO and SBAF use the same FIDO UAF protocol. SBAF adds electronic signature function using the extension of FIDO protocol.

5. Conclusion and Future Work

In this paper, we have suggested a secure biometric authentication framework system that combines with FIDO and PKI in a smartphone. This framework can be a solution to the problems caused by lack of user's identification and limitation of the

current FIDO service. By incorporating PKI's identification and FIDO's biometric authentication, this system would benefit everyone who wants to have a safe and convenient smartphone authentication environment.

References

[1] Y. Kim, Y. J. Park and J. Choi, "The Adoption of Mobile Payment Services for Fintech", International Journal of Applied Engineering Research, vol. 11, no. 2, **(2016)**, pp. 1058-1061.
[2] S. H. Lee and D. W. Lee, "A Study on Fintech Based on Actual Cases", International Journal of u- and e- Service, Science and Technology, vol. 9, no. 8, **(2016)**, pp. 439-448.
[3] M. Stokkenes, R. Ramachandra and C. Busch, "Biometric Authentication Protocols on Smartphones: An Overview", 9th International Conference on Security of Information and Networks, **(2016)**, pp. 136-140.
[4] S. R. Cho, D. S. Choi, S. H, Jin and H. H. Lee, "Passwordless Authentication Technology-FIDO", Electronics and Telecommunications Trends, **(2014)**.
[5] K. Nguyen, "Authentication and identification-Taking the user into account", Datenschutz und Datensicherheit – DuD, vol. 38, no. 7, **(2014)** July, pp. 467-469.
[6] G. Lyang Kim, J. Deok Lim and J. Nyeo Ki, "Secure user authentication based on the trusted platform for mobile devices", Journal on Wireless Communications and Networking, **(2016)** December.
[7] T. Thiemann, "Picking the right path to mobile biometric authentication", Biometric Technology Today, **(2016)** February, pp. 5-8.
[8] S. Machani, R. Philpott, S. Srinivas, J. Kemp and J. Hodges, "FIDO UAF Architectural Overview", FIDO Alliance, **(2014)** December.
[9] J. Jung Kim and S.-P. Hong, "Study on the Accredited Certification System without Password using FIDO", International Journal of Applied Engineering Research, **(2015)** June.
[10] Online Certificate Status Protocol, https://jamielinux.com/docs/openssl-certificate-authority/online-certificate-status-protocol.html.

Authors

Jae-jung Kim, received his BS degree in Computer Science from Chungnam University in 1997 and MS degree in Information Security from Korea University in 2003 respectively. He researched the information security for PhD at Sungshin University from 2009 to 2014. Since 1997, he stayed in LG-CNS Systems to develop PKI solutions and now he is working in Korea Information Certification Authority Inc. to research and develop FIDO based biometric authentication and vehicular PKI for autonomous driving car. His research interests include Public Key Infrastructure (PKI), cross certification, biometric authentication (FIDO), vehicular-PKI, and device authentication.

Seng-phil Hong, received his BS degree in Computer Science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched the information security for PhD at Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received Ph.D. degree in computer science from Korea Advanced Institute of Science and Technology (KAIST) in Korea. He is actively involved in teach and research in information security at The Sungshin Women's University, Korea. His research papers appeared in a number of journals such as ACM Computing, Springer-Verlag's Lecture Notes in Computer Science, etc. His research interests include access control, security architecture, Privacy, Smart Device Security and e-business security.