FIDO Alliance and Asia PKI Consortium White Paper: FIDO UAF and PKI in Asia – Case Study and Recommendations

Editor: Ms. Karen Chang, APKIC (Asia PKI Consortium)

Table of Contents

1. Development of PKI in Asia 4

1.1. Korea 5

1.2. Taiwan 7

1.2. Thailand 10

1.3. Macao 11

1.4. India 13

2. Case Study of FIDO and PKI 16

2.1. Korea K-FIDO (FIDO + NPKI certificate) by KISA 18

2.2. Taiwan Identification Center with PKI and FIDO by TWCA 20

2.3. Thailand Banking Service with PKI and FIDO 22

2.4. Macao eSignTrust eSignCloud with FIDO 23

2.5. India Aadhaar, PKI, and FIDO 25

3. Recommendations 28

3.1. Client side 29

3.2. Server side 31

4. Acknowledgements 38

5. References 38

Abstract

Adoption of FIDO (Fast Identity Online) standards has been rapid and universal. FIDO has become synonymous with secure e-authentication. In Asia, PKI (Public Key Infrastructure) retains a very important role to secure the trusted infrastructure in highly regulated sectors including financial, healthcare and government. The acceleration and the adoption of FIDO standards based on the existing PKI system would enable organizations to leverage their existing PKI infrastructure and provide a better user experience for PKI applications.

According to the practice of members of FIDO and the Asia PKI Consortium (APKIC), there are three possible scenarios covering FIDO deployment, all leveraging the FIDO UAF protocol. Scenario One is that FIDO is offered as a better *primary* authentication method and deployers would migrate PKI-based or other legacy authentication mechanisms to FIDO-based solutions. Scenario Two is that FIDO is offered as an alternative authentication method to provide better user experience. Scenario Three is FIDO offered to complement another protocol such as PKI-based protocol.

Scenario 1 is easier for designing new services from the scratch; otherwise, it would be a slow process. Scenario 2 & 3 will need to work with existing services. PKI services in Asia could be a good target for the second and the third scenario, that is, FIDO could provide an alternative authentication method in an existing PKI services or complement PKI with a better on-boarding process. Those areas could cover e-Identification, e-Authentication, and e-Transaction in Asian countries with national PKI/eID infrastructures and digital signature legislation.

From a technical aspect, there are three approaches to integrate FIDO UAF and PKI as required for scenarios 2 and 3. In this paper we name these approaches as Class 1, 2, and 3. For Class 1, only the authenticator is shared between FIDO and PKI; for Class 2, the registration process for FIDO and PKI are synchronized, either bootstrapped by each other or combined in one single sequence. For Class 3, the key pair between FIDO and PKI is shared.

This paper depicts the current or planned cases to integrate FIDO UAF and PKI in Asian countries and provides recommendations to consolidate the efforts among different works under the premise that the proposed approaches are compliant to FIDO's current standards.

1. Development of PKI in Asia

Many Asian countries/areas such as Korea, China, India, Taiwan, Thailand, Hong Kong, and Macau have legislated national PKI/eID infrastructure. APKIC represents the financial and the government sectors in the region to promote interoperability among PKIs in the region and to activate e-commerce utilizing the PKIs in the region.

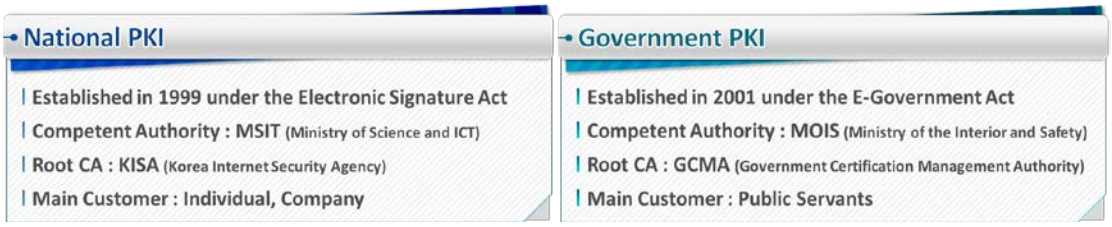
Table 1. Legislation and applications of PKI in Asia countries/regions

Country/ Region	National/Regional PKI	Digital Signature Legislation	Financial Regulation on PKI	eID and Other PKI Applications
China	✓ (Some regions)	✓ (ESL[1], 2005)	Mandatory for financial transaction above certain amount[2]	eID[3] (Optional, with PKI), e-Government, e-Commerce, etc.
Hong Kong	✓ (HKPost[4])	✓ (ETO[5], 2000)	Optional	eID[6] (Mandatory, with PKI option), e-Government, e-Commerce, etc.
India	✓ (CCA[7])	✓ (ITA-CCA[8], 2000)	Mandatory for high risk bank transactions	eID[9] (Mandatory, signed by PKI), e-Government, e-Commerce, etc.
Japan	✓ (JPKI[10])	✓ (ESaCBA[11], 2000)	Optional	eID[12] (Optional, with PKI option), e-Government, e-Commerce, etc.
Korea	✓ (NPKI, GPKI)	✓ (ESA[13], 1999)	Optional (Mandatory~2014)	eID (Optional without PKI) e-Government, e-Commerce
Macao	✓ (eSignTrust[14])	✓ (EDSL[15], 2005)	Optional	eID (Mandatory, with PKI option), e-Government, e-Commerce, etc.
Taiwan	✓ (GPKI[16], FPKI[17])	✓ (ESA[18], 2002)	Mandatory for high risk bank transactions[19] and all online stock trading[20]	eID[21] (Optional, with PKI), e-Government, e-Commerce, etc.
Thailand	✓ (NRCA[22])	✓ (ETA[23], 2001)	Optional	eID, e-Government, e-Commerce

In addition to Asia, the European Union's Regulation (EU) No 910/2014 on electronic identification and trust services (eIDAS[24]) went into effect on 1 July, 2016. eIDAS regulates electronic signatures, electronic transactions, involved bodies and their embedding processes to provide a safe way for users to conduct electronic transactions.

1.1. Korea

Korea has two kinds of PKI schemes. One is for individuals and companies, the other is for public servants in government. National PKI (NPKI) was established in 1999 under the Electronic Signature Act[13].



National PKI

| Established in 1999 under the Electronic Signature Act
| Competent Authority : MSIT (Ministry of Science and ICT)
| Root CA : KISA (Korea Internet Security Agency)
| Main Customer : Individual, Company

Government PKI

| Established in 2001 under the E-Government Act
| Competent Authority : MOIS (Ministry of the Interior and Safety)
| Root CA : GCMA (Government Certification Management Authority)
| Main Customer : Public Servants

Figure 1. National PKI and Government PKI in Korea

The competent Authority of NPKI is MSIT (Ministry of Science and ICT). KISA[25] has the role of the Root CA in NPKI. The NPKI certificates are issued to individuals and companies from the Accredited CAs and subscribers can also use their certificates to authenticate to online government services.

The government PKI was established in 2001 under the ‘E-Government Act’ and competent authority of this domain is MOIS (Ministry of the Interior and Safety). This domain issues the certificate only to public servants. They use GPKI certificates for their civil administration.

For the interoperability between NPKI and GPKI, the two domains are issued Certificate Trust List (CTL) separately.

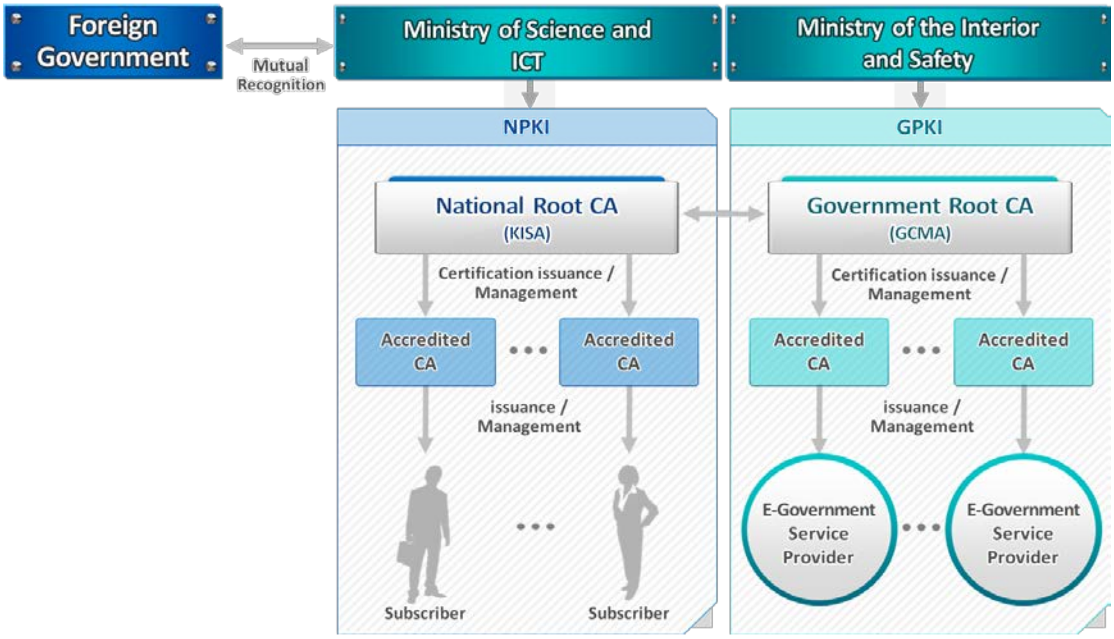

Foreign Government
Mutual Recognition
Ministry of Science and ICT
Ministry of the Interior and Safety
NPKI
GPKI
National Root CA (KISA)
Government Root CA (GCMA)
Certification issuance / Management
Certification issuance / Management
Accredited CA
Accredited CA
Accredited CA
Accredited CA
issuance / Management
issuance / Management
Subscriber
Subscriber
E-Government Service Provider
E-Government Service Provider

Figure 2. Interoperability of PKIs in Korea

Through 2016, the number of certificates issued by accredited CAs in NPKI is 35.45 million.

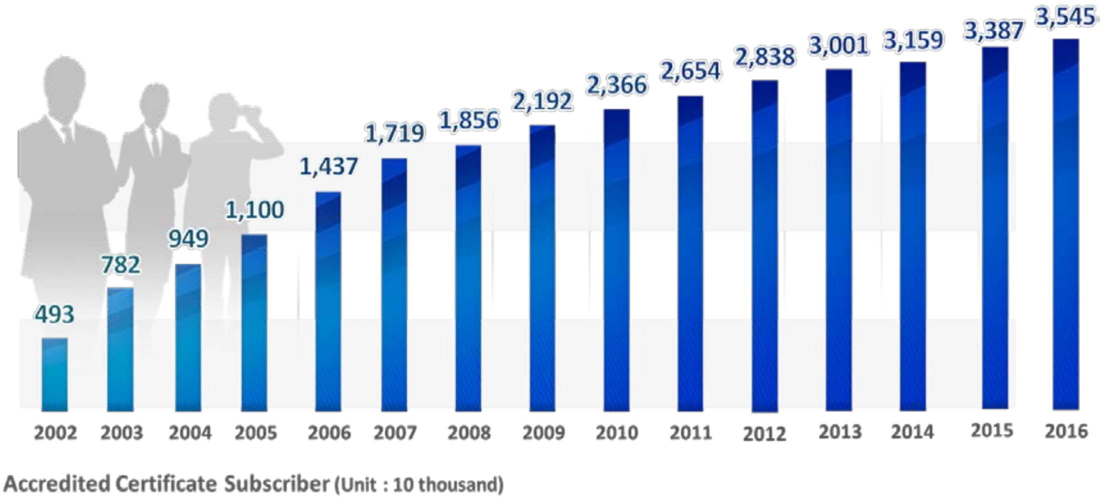
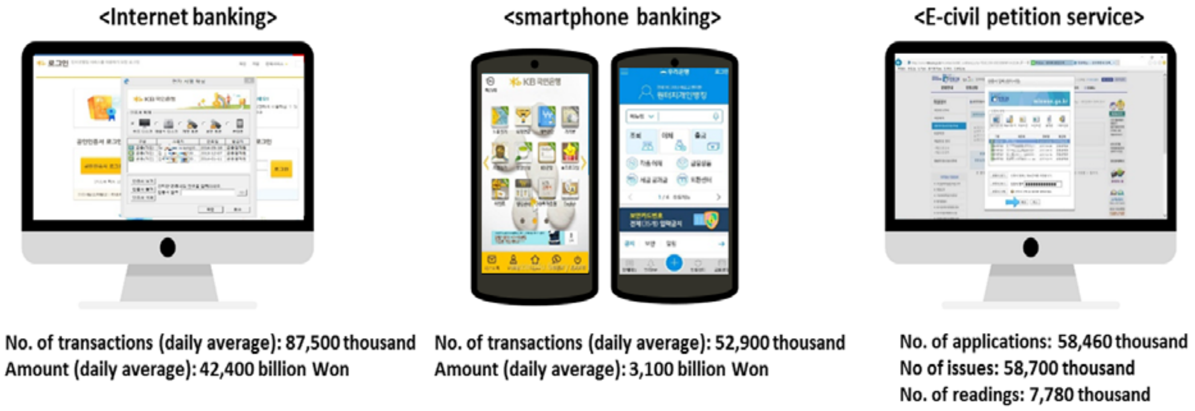


Figure 3. Number of certificate in NPKI of Korea[25]

NPKI certificates are widely used in internet banking, online stock trading, online shopping and e-government (G2C) services.



No. of transactions (daily average): 87,500 thousand
Amount (daily average): 42,400 billion Won

No. of transactions (daily average): 52,900 thousand
Amount (daily average): 3,100 billion Won

No. of applications: 58,460 thousand
No of issues: 58,700 thousand
No. of readings: 7,780 thousand

Figure 4. Applications of NPKI in Korea

1.2. Taiwan

Taiwan enacted the Electronic Signature Act[18] on November 14th, 2001. This act governs the legal status and use of electronic records and electronic signatures. Since then, the government and private sectors have been devoted to develop the PKI systems, especially in e-government and financial sectors.

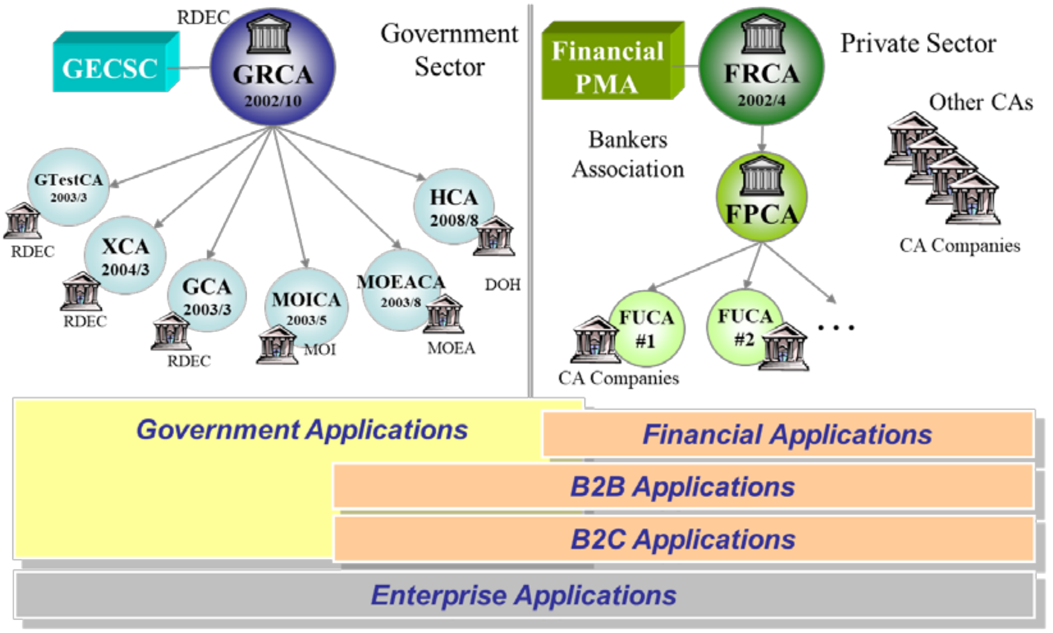


Figure 5. Overall development of PKI in Taiwan

1.1.1. Government PKI

Since the first government CA (GCA) started issuing certificates in 1997, Taiwan's Government Public-Key Infrastructure [16] (GPKI) has evolved into a hierarchical PKI, which comprises several CAs established by different ministries. Figure 6 below shows the CAs in the hierarchical structure of the Taiwan GPKI. The wide adoption of PKI technologies has not only enhanced information security of Taiwan e-government, but also provides greater efficiencies and carbon reduction.

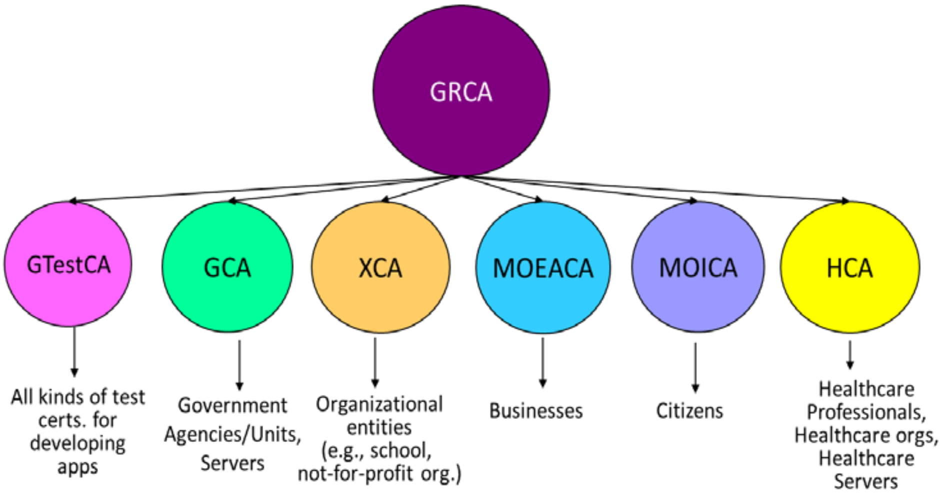

GRCA
GTestCA
GCA
XCA
MOEACA
MOICA
HCA
All kinds of test certs. for developing apps
Government Agencies/Units, Servers
Organizational entities (e.g., school, not-for-profit org.)
Businesses
Citizens
Healthcare Professionals, Healthcare orgs, Healthcare Servers

Figure 6. Hierarchical Structure of Taiwan GPKI

Among those CAs in Taiwan; GPKI, GRCA, GCA, MOEACA, MOICA [16], XCA, and GTestCA have been outsourced to Chunghwa Telecom [26]. All are established by using the HiPKI Certificate Management Suite developed by Chunghwa Telecom.

Smartcards issued by GPKI are able to support two-factor authentication and can replace traditional single factor, ID & password login. Moreover, the electronic signature and encryption mechanisms protect integrity, non-repudiation and the confidentiality of online transactions, and thus enhance information security. By replacing manual processes of signing paper documents with processes of electronic signing, improved efficiencies and a reduction in paper is realized. The number of smartcards issued by this product already exceed 4 million.

1.1.2. Financial PKI

In Taiwan, financial services (including cyber security, banking and insurance applications) play the most important role in private sector. The Taiwan Certificate Authority Corporation [27] (TWCA) occupies the largest portion in the financial market. Table 2 depicts key milestones of the TWCA.

Table 2. Milestones of Taiwan's Financial PKI

Milestones	
DEC.1999	Under the consent of Financial Ministry, TWSE (Taiwan Stock Exchange Corporation), FISC (Financial Information Service Corporation), TRADEVAN (Trade-van Information Services Corporation),TDCC (Taiwan Depository & Clearing Corporation) and other excellent civic information corporations together to prepare to establish Taiwan Certificate Authority Corporation (TWCA)
APR.2002	Openly recommended by the banking association of Taiwan, TWCA manages Financial Root CA in Taiwan
AUG.2002	TWCA is the first legal Certificate Authority awarded by the Commercial Department of Economic Ministry
SEP.2002	Root CA in Taiwan was completed
SEP.2002	FRCA started operation
OCT.2002	The CPS of FRCA was approved by the Commercial Department of Economic Ministry
MAY.2004	Conducted financial certificate service for i-tax system
JUN.2007	Awarded the ISO27001 certification for all CA system by the British Standards Institute (BSI)
MAY.2009	Awarded the WebTrust certification
JAN.2015	Provided Insurance e-policy third party authentication and validation service (ISAV)
MAY.2015	Supported TDCC i-voting service with TWID app
DEC.2015	Launched QRDV service to produce and validate safe QR code including e-signature from trusted parties
NOV.2016	Announced TWID platform with Financial Supervisory Commission (FSC) to provide online authentication service
MAR.2017	Under the approval of the Ministry of the Interior to promote the MOICA natural person certificate verification service
MAY.2017	Cooperated with Taiwan Clearing House (TCH) to provide online bank account linking service for securities company

TWCA laid the foundation of PKI by securities and banking businesses initially, and developed more usages including insurance, i-voting, i-tax, etc. Some government services have also started to adopt private certificates, including i-tax.

Many service providers are eager to identify new users online, but the methods undertaken are limited. Currently, all users must apply for a personal certificate in person in a branch office. The issued certificates are necessary for online service providers to identify new users.

TWCA also provides entities an online authentication solution, which supports multiple factors including e-ID, national health cards, debit cards, etc. With this solution, financial institutions could adopt several factors to identify new users online with much greater ease and rigor.

The 2016, TWCA has issued 4.2 million certificates in the private sector.

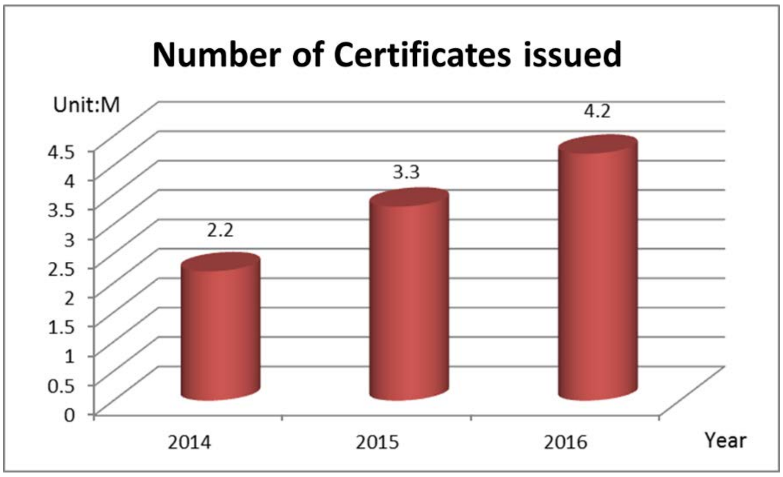


Figure 7. Number of Certificates issued by TWCA

1.2. Thailand

Entering the digital era is a global trend. It is evident that the global economy is being driven by technological advances and a shift towards increased use of online platforms. With an increase in online activities, strong government support and improvements in digital infrastructure, Thailand is undergoing an enormous transformation to become a digital economy with the widespread use of mobile devices as well as significant growth of e-government services, e-commerce markets and e-payment systems.

The government of Thailand's Department of Provincial Administration (DoPA) issues the Thai National ID Card, an official document used for proof of identity. In addition to displaying basic information about the cardholder, the Thai National ID Card also stores personal data on its cryptographic chip in electronic form. The Thai National ID Card is widely used for conducting governmental and business transactions including accessing public services, establishing a business, and opening bank accounts.

The demand to conduct financial transactions with mobile devices has increased dramatically because users can conveniently shop via a mobile device. However, user convenience must be balanced with appropriate security and authentication. Certain transactions require a legal digital signature based on Public Key Infrastructure (PKI) technology. Therefore, there is a need to authenticate mobile users to securely conduct transactions with mobile devices.

For greater convenience, public and private sectors are searching for the best technology to achieve both purposes. FIDO is one technology that can potentially address these requirements as it can provide convenient and secure authentication.

However, certain transactions require a legally binding legal digital signature based on PKI technology. Internet transactions would be much more convenient if a mobile phone could be used for the purpose of authentication and a digital signature. For greater convenience, public and private sectors are searching for the best technology to achieve both purposes. FIDO is the technology that can potentially and meet the above requirements as it can provide convenient and secure authentication.

1.3. Macao

CTT eSignTrust Certification Services[14] (eSignTrust) is Macao's first and currently the only Certificate Authority (CA) accredited by the Macao Special Administrative Region (MSAR). eSignTrust is managed by Macao Post and Telecommunications Bureau[28] (CTT) in accordance with Electronic Documents and Signatures Law[15] (EDS Law) of MSAR (Law No 5/2005 of MSAR).

According to EDS Law, the following types of signature and certificate are defined:

- **Advanced Electronic Signature (AES)** is an Electronic Signature that is uniquely linked to the signatory, is capable of identifying him, is created using means that he can maintain under his sole control and is linked to the data to which relates in such a manner that any subsequent change of the data is detectable. According to the EDS Law, an Electronic Document signed with an AES has legal effectiveness, which is evaluated according to the general legal rules and the agreement of the involved parties.

- **Qualified Electronic Signature (QES)** is an Advanced Electronic Signature based on a Qualified Certificate. According to the EDS Law, an Electronic Document that can be represented as a written statement, signed with a Qualified Electronic Signature, has full evidentiary value of the declarations attributed to its signatory.
- **Electronic Signature (ES)** is data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. The EDS Law provides legal support for the electronic signature.
- **Qualified Certificate** issued by eSignTrust provides a very high degree of assurance of a certificate holder’s identity for his/her private or professional electronic identity. Its corresponding key pair is generated and contained in a Secure Signature-Creation Device (SSCD). The main usage of eSignTrust Qualified Certificate is to create QES. Another usage of eSignTrust Qualified Certificate is to provide additional factor of authentication by e-Banking. [29]

The eSignTrust CA issues digital certificates to natural individuals, users of organizations and government bureaus at three levels of distinctive credibility. Credibility of the certificate depends on enforcement of subscriber’s identity verification procedures and the effort used by eSignTrust to verify the data submitted by the requester in his/her/its registration application. The higher strength and complexity of the level of the security, the higher level of credibility is achieved and assigned.

eSignTrust launched eSignCloud Service to provide a safe, reliable and user-friendly online signing tool capable of providing real-name authentication for government departments, business organizations and individual users. eSignCloud Service enables users to sign electronic documents on mobile devices anywhere and anytime alongside its security, convenience and legal effectiveness.

“eSignCloud” is a AES-based signature service. It is designed to allow easy integration for Online applications to be upgraded to be eSignable web applications enabling real-name authentication of signers’ identities and stronger legal value. The enhanced security and convenience of eSignCloud Service is of benefit to boost the confidence of the public regarding online services and transactions.

eSignCloud Service requires users to create an account with their AES certificate, and can be used in conjunction with the free eSignTrust Mobile One-Time Password (eSignTrust MOTP) mobile application to enable two-factor authentication for stronger protection.

To further enhance the eSignCloud Service, eSignTrust intends to have the following aspects:

- Comprehensive model for signature rules and policies
- Enhancement on authentication mechanism (fingerprint, NFC, Smart ID Card, etc)
- Support for full range of signature profiles
- QES-based eSignCloud
- Cross-border legal recognition and remote authentication registration process
- Trust Services Infrastructure for e-Identification, e-Authentication, e-Signature and related services

1.4. India

Electronic Identification and Authentication services in India have matured over the last 15 years. In recent years, the government has put more thrust on paperless, cashless and presence-less services and is encouraging policies and innovations around it.

The law for electronic records and electronic signatures[8] was passed in India in 2000. This gave a legal backing for IT revolution in the country. This was also a mandate from the United Nations' Cross-Border electronic trade facilitation program. The early adoption of electronic authentication started for Import and Export systems in India.

While electronic records were an initial movement, the digital/electronic signatures took prominence in 2004-05 while company law boards of India introduced electronic facilitation of filings. Further income yax filing have brought digital adoption to a larger population since 2006-07. Eventually, electronic authentication embraced larger implementations like in eProcurement systems, railway booking agents, GST filing systems, government-to-citizen services, etc.

In the year 2011-12, India introduced its state of the art National ID system named 'Aadhaar' [9]. This is a unique card-less identity given to every resident of India in the form of a 12 digit unique number after enrollment of such person with their demographic and biometric information. This is a highly secured and structured system with large scale acceptance. Today, 1.17 billion people in India are already covered in this program (more than 95% of the total population).

The unique thing about Aadhaar is its card-less behavior. The original copy of Aadhaar is also issued electronically (PKI based Digitally Signed PDF), which can be used directly in any authentication system. On the other side, governments, banks and other regulated agencies are allowed to gain secure connectivity to perform online verification of their users directly with Aadhaar. This online service is secured with PKI source-encryption and signed with a tamper-proof transaction model. Using this server, users can authenticate themselves by keying in their 12 digit Aadhaar plus authentication factor.

In the year 2015, India launched world's largest electronic signature (eSign) program by amending its Information Technology Act[8]. This eSign is backed by the Aadhaar system and allows users to sign on the fly. This facilitated a large number of platforms to easily adopt PKI for identification, authentication and signing processes in an online form. Today, banking and government systems are enabled to use eSign and facilitate paperless, and presenceless services.

eSign has been widely adopted and currently has more than 20 million users, which is nearly 2% of the country's population. It also facilitates more than 200,000 transactions per day through computers and mobile devices.

1.4.1. Applications

In India, online systems are increasing day by day. Below are the key online applications which citizens are required to use:

1. Banking & Financial websites Applications
2. eCommerce websites / applications
3. Tax filing websites
4. Enterprise or Retail Customer login websites / apps
5. Government to Citizen services
6. E-Tendering Websites

7. Entertainment / Movie tickets
8. Airlines & Railway websites / apps

1.4.2. Authentication Mechanisms

All these systems have devised their own authentication techniques. The Majority of them use Username + Password systems. Some of them also have One Time Password authentication either as primary factor or a second factor. In addition to this, PKI has played a crucial role in fulfilling secure authentication gaps over the last decade. In several banking systems, PKI is a second factor authentication for corporate fund transfers. When it comes to government platforms like e-Tenders, PKI plays important role in primary authentication as well as encryption of data. In the recent past, Aadhaar has also become an easy to adopt (Open API) authentication model for most modern systems.

1.4.3. Developing Trends

Aadhaar is one of the most critical developments in India where government emphasis continues for larger adoption in identification of citizens. Most of the Aadhaar data has a registered mobile and email ID, along with authenticed demographic information and photographs. Hence, it is being adopted to provide authorized access for online authentication / KYC using Biometric / OTP based verification.

India is also known for its large and sophisticated national Public Key Infrastructure (PKI). While this is highly regulated, the National PKI setup comprises of 4 public certifying authorities and 3 close-group certifying authorities, all regulated by the Indian government. The certificates under this PKI are trusted by Adobe, Microsoft and other platforms which have PKI based user software. India also has a large user base of PKI. There are more than 15 million long term digital signatures issued and used across several applications. With the recent innovations, electronic signatures have crossed 20 million users, which helps any new system to adopt it easily with Open APIs regulated by government. The recent Goods and Service Tax (GST) system is also one of the largest users of PKI to help nearly 10 million users to interact & file electronically.

2. Case Study of FIDO and PKI

FIDO is by far the world's largest ecosystem for standards-based, interoperable and pluggable authentication based on public key cryptography. FIDO is suitable for providing better security of online services while also reducing cost for the enterprise because it is compatible with most mobile devices and browsers. The overall process is simple and more secure for consumers than legacy solutions.

Although FIDO and PKI are based on public key cryptography, they take different approaches. FIDO makes the protocol applicable to various vertical solutions that require user authentication. It is focused on ensuring the user's privacy and uses public cryptography method to authenticate the user to a Relying Party. Credentials are guarded by user verification (e.g. biometrics based or PIN based) and they are typically stored securely within on-device secure element. The biometric verification is only required on the client side to perform local authentication in order to unlock the private key for conducting the cryptography calculation. The user's biometric data will never leave the device, thus sharing only the essential information with the authentication server and the relying party during authentications. The user, key pair and the relying party are a tuple which means FIDO uses one key pair per relying party and avoids the usage of a global correlation handle. The design principle of the FIDO protocol does not allow tracking users' behavior across multiple relying parties[1]. The Identity binding required to be performed is outside FIDO's scope and can be implemented according to the demand or regulations.

PKI systems, on the other hand, address the needs of digital signature legislation with the involvement of trusted third parties, such as Certificate Authorities (CA), Registration Authorities (RA), and Validation Authorities (VA). In addition, PKI also includes a set of policies and procedures to create, manage, distribute, execute, store process as well as when revoking digital certificates or managing public key encryption. The revocation and validation of certificates is required as one certificate is relevant to multiple relying parties. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking, electronic government, etc.

[1] There still exist tracking methods (such as Cookies, etc.) that could be used outside of the FIDO protocol to track user's behavior.

Due to the complexity and the practical issues when deploying PKI solutions, the identity federation service emerges and it aims at solving the trust anchor issues. However, identity federation works better within a small trust circle composed by already known parties where the definition of identity context is clear and similar across all the parties. For example: an identity federation service for banking allows a user to identify himself to other banks, as the context of identity provided by the user can easily mapped to another bank for identification purpose.

While PKI tries to create globally recognized credentials with specified attributes, it is suitable to combine PKI with an identity federation service. Also, a PKI enabled root of trust can easily integrate into an identity federation service to enlarge the existing trust circle and augment the weak trust relations. As for individual relying parties who want to have fine-grained profile of a specific user, FIDO can be complemented with a PKI ecosystem to ensure there exists a strong and standardized identity binding across relying parties. We have depicted the identification and authentication flow below:

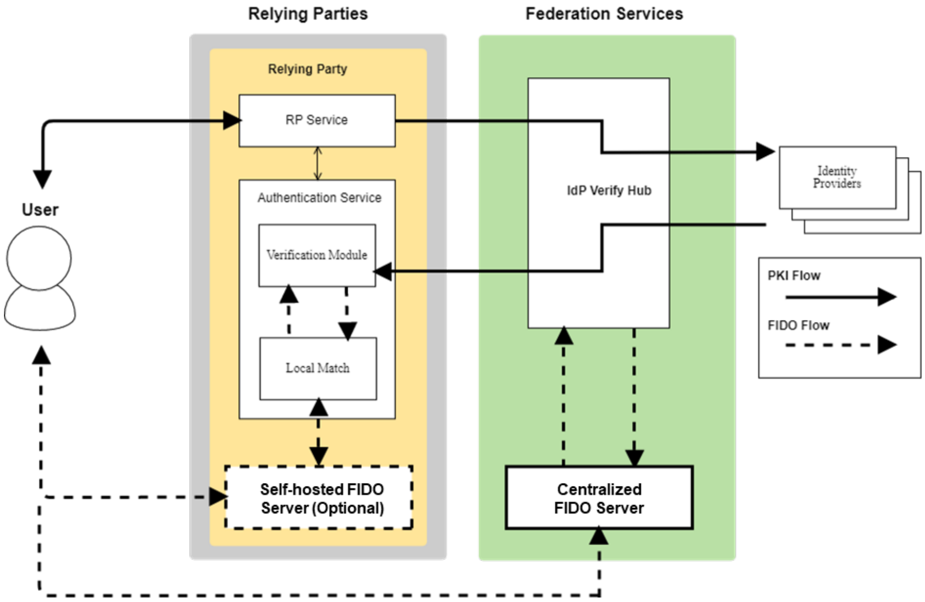


Figure 8. Identity Federation Flow

A user accessing an RP service will be asked to provide his PKI credential and proof of possession of the private key to the RP Service first. The RP Service will then hand over the credential to the IdP Verification Hub. The credential will be forwarded to Identity Providers such as Telecom, Banking or Government IdPs depending on which kind of PKI the user possesses. A FIDO Server can be deployed in a centralized manner by a PKI provider or self-hosted by the relying party. The difference between these two deployment models will depend on business requirements, user experience and regulatory compliance.

An RP that wants to enhance the user experience can opt to use FIDO as the primary authentication method after an initial identity binding step based on PKI identification (with a self-hosted FIDO server). In this way, the overall PKI authentication time is reduced and the user can perform the authentication on their smartphones naturally and seamlessly. In short, PKI provides the fundamental root of trust and general attributes of a user while FIDO can complement this with such foundations and even enhance the performance and user experience by its standard-based security requirement as well as the enforcement of solution certification processes.

Since both FIDO and PKI are based on the same public cryptography, it's possible to share the common cryptographic component between a FIDO and PKI system in which the approach will not violate FIDO's privacy principle and the security requirements for cryptographic keys are met, including key sizes, crypto algorithms, key generation procedure, key protection, etc.

2.1. Korea K-FIDO (FIDO + NPKI certificate) by KISA

As the importance of online life grows, it is required to provide the online means that plays the role of identification (resident card) and signature (seal, autograph, etc.)

Table 3. Status of Online and Offline authentication in Korea

	Online	**Offline**
Relevant law	Digital Signature Act	Resident Registration Act
Proof of act	Identification + Digital signature (Certificate)	Resident card + Seal (Autograph)

Accredited certificates are used as a security means to confirm identity, to prevent tampering of electronic documents, and to confirm authenticity of online transactions.

With the recent change of ICT environments from wired to mobile devices there is an increased requirement to provide the means for the convenient, secure, and easy to use accredited certificates.

The K-FIDO[25][30] technology enables users to use certificates by using the registered biometric data without entering passwords and ActiveX installation. In order to minimize changes of the FIDO standard, FIDO and a certificate link technology framework is added to the FIDO UAF[31] framework. That is why the K-FIDO technology uses a separate public key pair for user authentication and digital signature, if necessary, for the applications which are using NPKI certificates.

K-FIDO technology makes a link with certificates by using an extension message without changing the FIDO structure or UAF protocol.

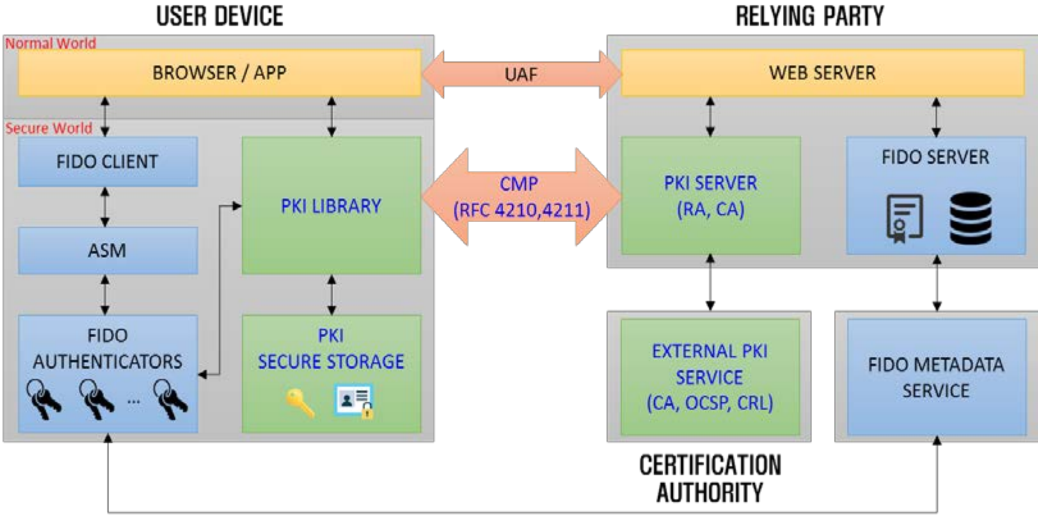


Figure 9. Overview of K-FIDO

The FIDO authentication technology enables users to use certificates by using the registered biometric data without entering passwords (using PKCS#5 and #8 specifications).

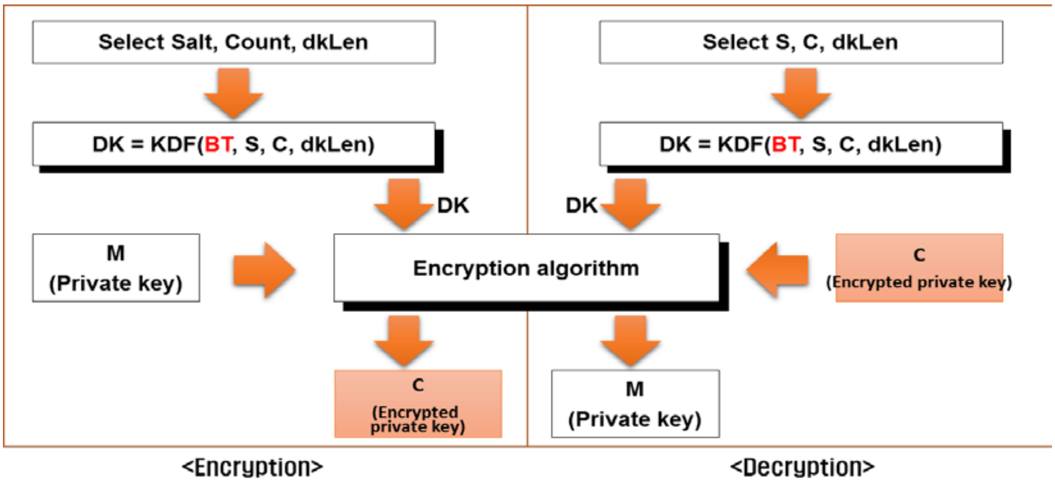


Figure 10. Protecting the key pairs of PKI with biometrics

Currently, K-FIDO technology has been applied in some mobile banking services by using the registered biometric data such as fingerprint and iris.

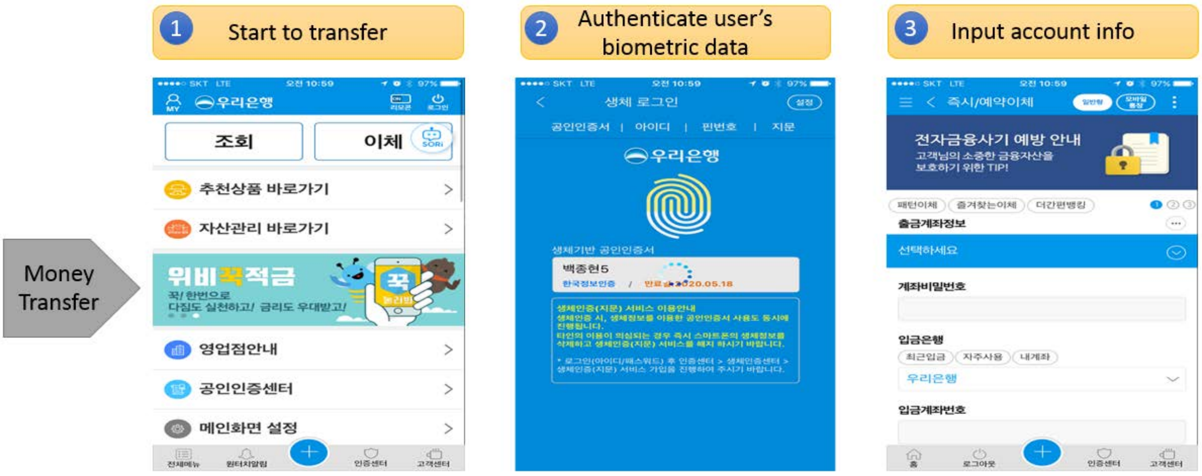


Figure 11. Applications of K-FIDO

2.2. Taiwan Identification Center with PKI and FIDO by TWCA

TWCA provides security solutions with PKI technology to the financial industry, including bank, stock security companies, securities investment trust & consulting companies, government agencies, etc. Currently users need to enable certificates with password. TWCA hopes to improve user experience with a FIDO solution. TWCA will integrate a CA component and a FIDO UAF component, which will help users to enable certificates with the local authentication function from FIDO UAF. FIDO's local authentication function has adopted multiple biometric technologies already so users can enable certificates more easily with their fingerprint, iris or other biometrics.

TWCA has also developed more online authentication methods. Users could use e-ID, bank account and other tools to apply certificate online with TWCA's ID service. TWCA provides single portal to institutional clients to connect with multiple ID partners, and then end users can input their ID information online through TWCA's service to identify themselves.

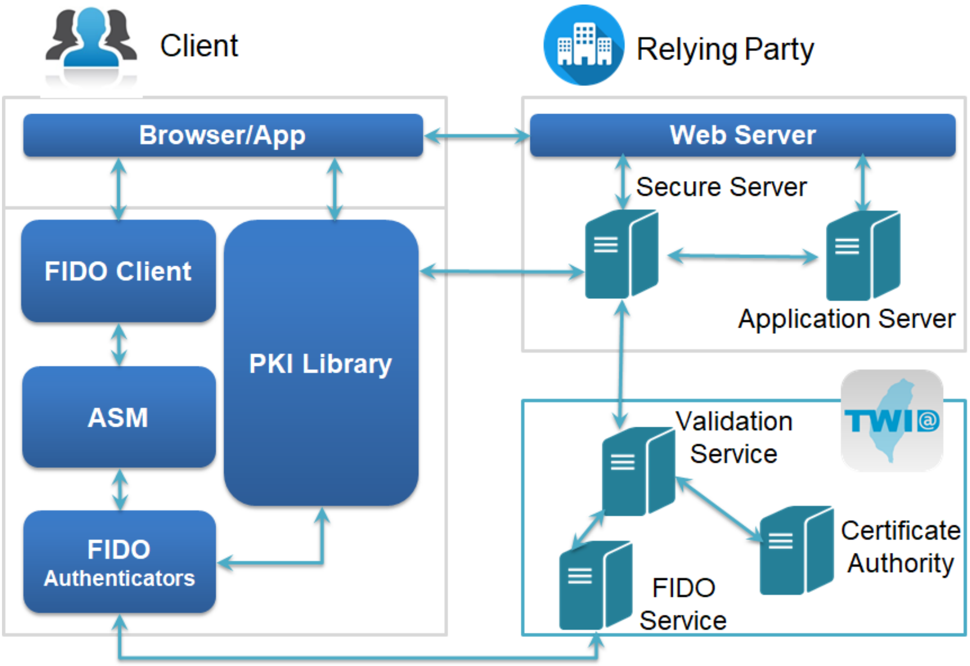


Figure 12. Overview of FIDO and PKI by TWID

TWCA started the TWID platform which develops more applications with partners, and the certificate can be applied to multiple applications with the TWID app. For example, certificates can be applied for e-voting and to query personal investment records from TWSE (Taiwan Stock Exchange) and TFE (Taiwan Future Exchange).

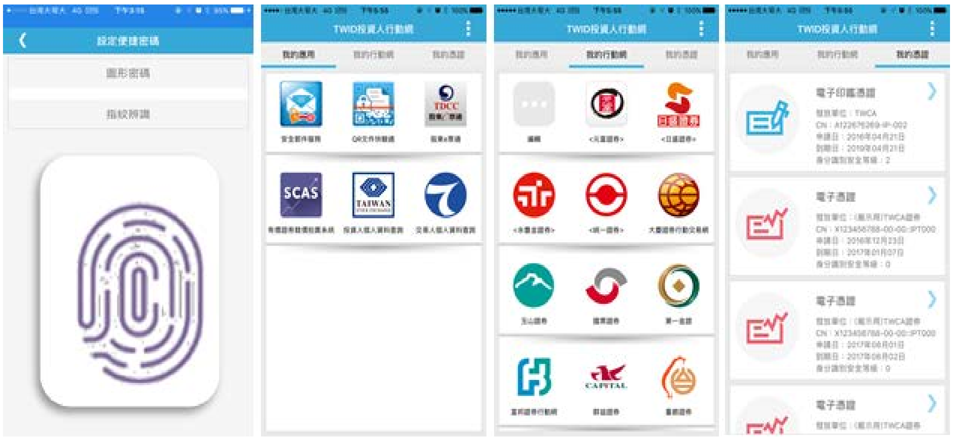


Figure 13. Applications of TWID

2.3. Thailand Banking Service with PKI and FIDO

In the diagram below, a bank customer must register a mobile phone in person to enroll in the public key system and acquire a certificate at a local bank branch. Subsequently, the customer can use a mobile phone to authenticate banking transactions and document signing.

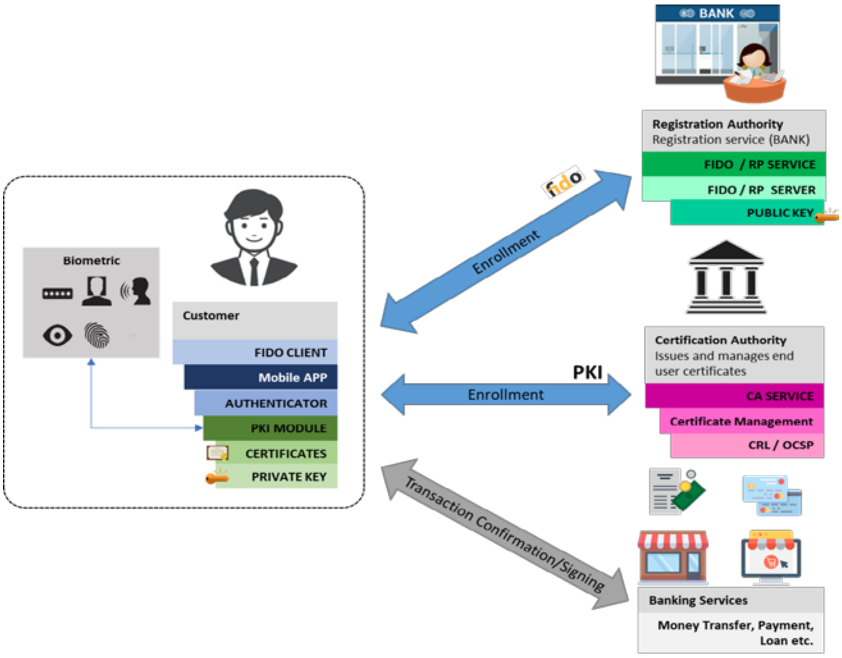
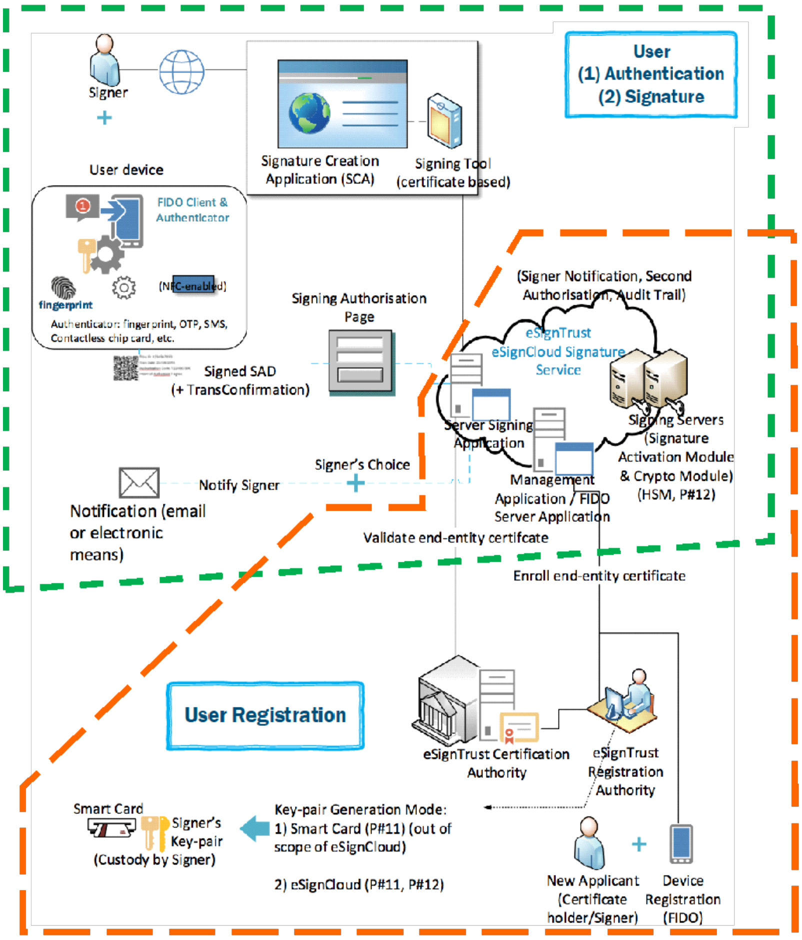


Figure 14. Integration of PKI and FIDO in Thailand

2.4. Macao eSignTrust eSignCloud with FIDO

The figure blow demonstrates how to integrate Macao eSignTrust eSignCloud Service with FIDO.



User
(1) Authentication
(2) Signature
Signer
User device
Signature Creation Application (SCA)
Signing Tool (certificate based)
FIDO Client & Authenticator
fingerprint
(NFC-enabled)
Authenticator: fingerprint, OTP, SMS, Contactless chip card, etc.
Signing Authorisation Page
Signed SAD (+ TransConfirmation)
(Signer Notification, Second Authorisation, Audit Trail)
eSignTrust eSignCloud Signature Service
Server Signing Application
Management Application / FIDO Server Application
Signing Servers (Signature Activation Module & Crypto Module) (HSM, P#12)
Signer's Choice
Notify Signer
Notification (email or electronic means)
Validate end-entity certifcate
Enroll end-entity certificate
User Registration
eSignTrust Certification Authority
eSignTrust Registration Authority
Smart Card
Signer's Key-pair
(Custody by Signer)
Key-pair Generation Mode:
1) Smart Card (P#11) (out of scope of eSignCloud)
2) eSignCloud (P#11, P#12)
New Applicant (Certificate holder/Signer)
Device Registration (FIDO)

Figure 15. Integration of eSignTrust eSignCloud Service with FIDO

- **User Registration Process:**
  1) eSignCloud requests authorization via Gov. IdP (authz server)
  2) eSignCloud gets assess token from Gov.IdP and creates eSignCloud account using access token info
  3) eSignTrust RA enrolls for a eSignCloud certificate from eSignTrust CA

4) User logs into eSignCloud to initiate registration of FIDO and signer’s signature activation data

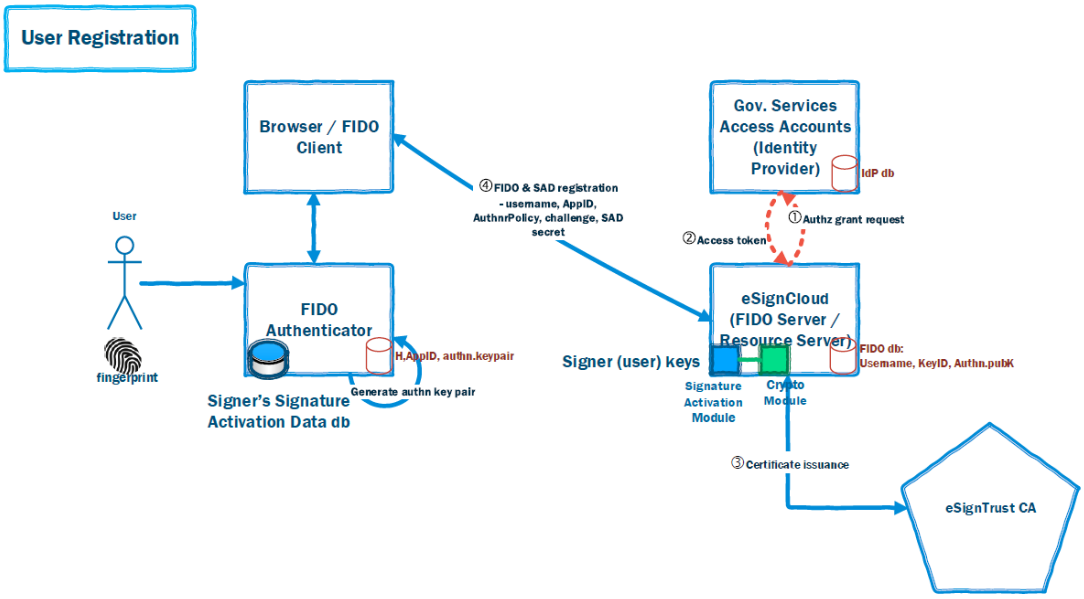

User Registration
Browser / FIDO Client
Gov. Services Access Accounts (Identity Provider)
IdP db
④FIDO & SAD registration - username, AppID, AuthnrPolicy, challenge, SAD secret
①Authz grant request
②Access token
User
FIDO Authenticator
fingerprint
H,AppID, authn.keypair
Generate authn key pair
Signer’s Signature Activation Data db
eSignCloud (FIDO Server / Resource Server)
Signer (user) keys
FIDO db: Username, KeyID, Authn.pubK
Signature Activation Module
Crypto Module
③Certificate issuance
eSignTrust CA

Figure 16. User Registration Process of FIDO and eSignTrust eSignCloud Service

- ■ **User Authentication and Signing Process:**

1) (optional) User logs into SP application

2) (optional) SP authorization grant process:

   a. SP sends authorization request to IdP (Gov.Services)

   b. SP redirects user agent to IdP (Gov.Services) provide authentication

   c. User agent gets authentication code from IdP (Gov.Services)

   d. User agent sends authentication code to SP

   e. SP get access token by authentication code

3) User requests signing service, then SP computes DTBS (Data To Be Signed) and sends it to eSignCloud

4) eSignCloud FIDO Server sends FIDO authentication request to FIDO Client. FIDO Client gets FIDO Client’s private key access right through FIDO Authenticator. If successful, then FIDO Client will sign the Signature Activation Data (SAD) by FIDO

Client's private key and sends the authentication response including SAD back to eSignCloud.

5) eSignCloud Signature Activation Module verifies SAD and activates signing to Crypto Module. eSignCloud sends Signature Value to SP

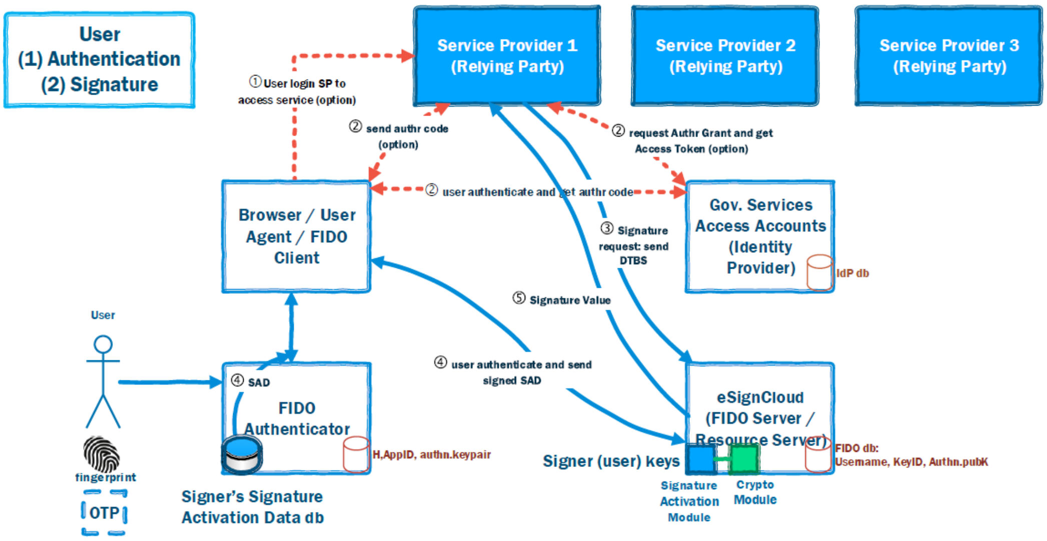

User
(1) Authentication
(2) Signature
Service Provider 1
(Relying Party)
Service Provider 2
(Relying Party)
Service Provider 3
(Relying Party)
① User login SP to access service (option)
② send authr code (option)
② request Authr Grant and get Access Token (option)
② user authenticate and get authr code
Browser / User Agent / FIDO Client
Gov. Services Access Accounts (Identity Provider)
IdP db
③ Signature request: send DTBS
⑤ Signature Value
User
④ user authenticate and send signed SAD
④ SAD
FIDO Authenticator
H,AppID, authn.keypair
eSignCloud (FIDO Server / Resource Server)
FIDO db:
Username, KeyID, Authn.pubK
Signer (user) keys
fingerprint
OTP
Signer's Signature Activation Data db
Signature Activation Module
Crypto Module

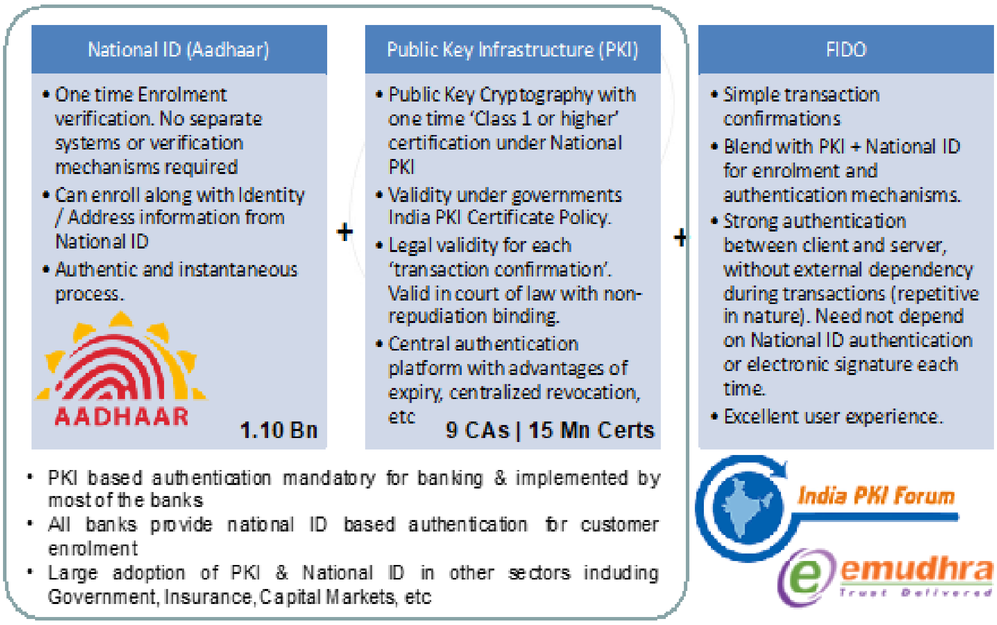
Figure 17. User Authentication and Signing Process of FIDO and eSignTrust eSignCloud Service

2.5. India Aadhaar, PKI, and FIDO

Aadhaar and other identity platforms currently support an identity proofing aspect for several transactions. In organizations like banks or businesses, they have their own verified user base. Hence, they can easily expose a simpler identity proofing system within their database by exposing questions / seeking information. These all can provide the necessary identity proofing support that FIDO requires for initial registration.

The PKI system plays its own role for identity backed signature, data encryption, legal binding, non-repudiation, revocation and other requirements of the systems as well as legal regulations.

FIDO can play a vital role in fulfilling the need of user authentication within those systems. Such user authentication / validation is a repeated activity, and currently the systems rely on alternates where most of them are online. This exposes a dependency and risk as the demographic information or the authentication parameters have to repeatedly travel over the internet. FIDO brings a key strength of authenticating the user locally, as well as fulfilling the security requirements required by such systems.



National ID (Aadhaar)

- One time Enrolment verification. No separate systems or verification mechanisms required
- Can enroll along with Identity / Address information from National ID
- Authentic and instantaneous process.

1.10 Bn

+

Public Key Infrastructure (PKI)

- Public Key Cryptography with one time 'Class 1 or higher' certification under National PKI
- Validity under governments India PKI Certificate Policy.
- Legal validity for each 'transaction confirmation'. Valid in court of law with non-repudiation binding.
- Central authentication platform with advantages of expiry, centralized revocation, etc

9 CAs | 15 Mn Certs

+

FIDO

- Simple transaction confirmations
- Blend with PKI + National ID for enrolment and authentication mechanisms.
- Strong authentication between client and server, without external dependency during transactions (repetitive in nature). Need not depend on National ID authentication or electronic signature each time.
- Excellent user experience.

- PKI based authentication mandatory for banking & implemented by most of the banks
- All banks provide national ID based authentication for customer enrolment
- Large adoption of PKI & National ID in other sectors including Government, Insurance, Capital Markets, etc

Figure 18. Concept for Integration of Aadhaar, PKI and FIDO in India

To support these concepts, FIDO Alliance has established the FIDO India Working group, and that working group and some Indian Certificate Authorities have discussed FIDO possibilities in several banking systems and other authentication platforms.

For any new or existing system to adopt FIDO authentication, co-existence with current methodologies is the key. Along these lines, the strengths of each method need to be considered as indicated below:

- ID Proofing with the use of existing system
  - Users are on-boarded to system using the conventional models of the organization.
  - This is a one-time enrolment verification. No separate systems or verification mechanisms are required.
  - National ID (Aadhaar) can also be used to enroll along with Identity / Address information.
  - This makes it Authentic and is an instantaneous process.
- Public Key Infrastructure (PKI)

    - Public Key Cryptography with one-time certification under National PKI
    - Validity under governments India PKI Certificate Policy
    - Legal validity for each 'transaction confirmation'. Valid in court of law with non-repudiation binding
    - Central authentication platform with advantages of expiry, centralized revocation, etc
- FIDO
    - Simple transaction confirmations
    - Blend with PKI + National ID for enrolment and authentication mechanisms
    - Strong authentication between client and server, without external dependency during transactions (repetitive in nature). Does not depend on National ID authentication or electronic signature each time
    - Excellent user experience

3. Recommendations

From past experience as well in looking at on-going market trends, we would like to identify how FIDO UAF can support existing PKI systems and how PKI could expand adoption of FIDO authentication. These two technologies share lots of similarities in that they both use public key cryptography, but there some differences also exist. Most of the difference is that PKI provides a globally recognized credential while FIDO UAF has scoped key pairs upon each relying party. Additionally, PKI can be seen as more complicated to implement and to obey the overall policy. Our focus here, however, is not to talk about which solution will dominate the market – but rather to consider how these two technologies can work together to bring innovation to the authentication marketplace and to pave the way for deploying better authentication solutions to the public. Based on the Case Study above, we can classify three major classes to integrate FIDO UAF and PKI, they are:

- Class 1: Shared authenticator: Our Class 1 refers to a shared authenticator scenario where both FIDO UAF and PKI credentials are stored in a common device (e.g., a shared cryptography module with separated key storage). The purpose of Class 1 is to look at things from a manufacture's perspective and also to consider the convenience of users with one single device to support both FIDO and PKI. The core concept is that since both FIDO and PKI are built upon Public Key Cryptography – so fundamentally there is a need for some components to be shared across these two protocols.
- Class 2: Synchronized Registration Process: In Class 2, we propose to synchronize the registration by bootstrapping or combining the registration process of FIDO UAF or PKI with each other. This is the concept referenced from the derived "Personal Identity Verification" (PIV) credential model of NIST standards[32], to leverage the existing PKI credential to bootstrap FIDO's approach with better usability and user experience for authentication, or to issue certificates to existing FIDO users for digital signing purposes. In this class we have three approaches in the registration process:
    1. (1) If the user already has a valid PKI credential, use it to bootstrap the FIDO UAF registration process.
    2. (2) If the user already has a valid FIDO UAF key pair, use it to bootstrap the registration process of PKI.
    3. (3) If the user is new for both FIDO UAF and PKI, then the registration process of FIDO UAF and PKI are combined into one single sequence.

After the registration process above, the user will have credentials for both FIDO UAF and PKI with different key pairs. The user can use them independently according to the requirement of the applications.

- Class 3: Shared key pair: In this Class, PKI will reuse a FIDO UAF key pair, or generate a new key pair for both FIDO UAF and PKI.

Class 1 and 2 could be implemented by extension of the FIDO UAF specifications, as detailed in the following sections. For class 3 it may conflict with FIDO Security Guidelines[33]: if PKI re-uses the FIDO UAF key pair, or FIDO UAF and PKI generate the same key pair in the registration process, then this key pair will not be specific to a single Relying Party, which will conflict with SM-2 in sec. 5 of FIDO Security Guideline.

As a consequence, the usage of Class 3 will need to consider the relation between the user, a Certificate Authority and a Relying Party in more detail. In this white paper we only focus on Class 1 and Class 2, and leave Class 3 for further discussion in the future.

3.1. Client side

For all classes there are two different approaches on the end device: either PKI shared cryptography module with FIDO Authenticator or in the opposite way. This is described further in the following sections.

3.1.1. PKI use FIDO's authenticator

As depicted in Figure 19, on the left side is a proposed architecture for PKI use of FIDO's authenticator as a shared cryptography module. The right side depicts the defined components and corresponding APIs.

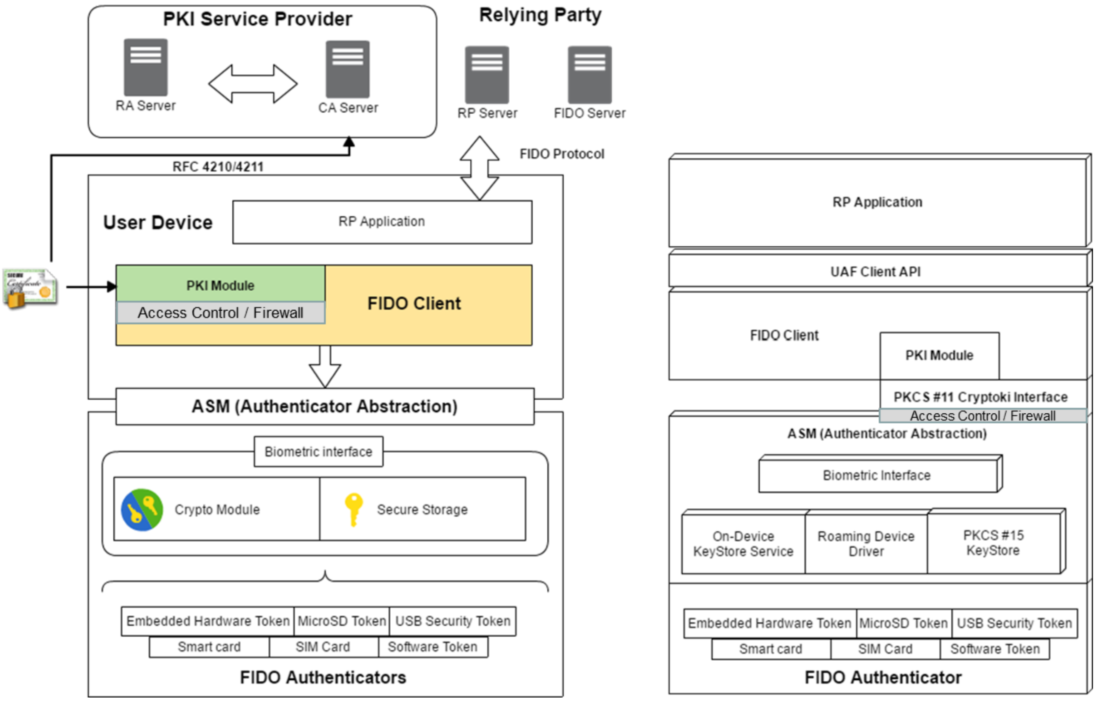


Figure 19. PKI use FIDO's authenticator

A FIDO Client will have an embedded PKI module which may directly or indirectly communicate with an RP Application depending on the implementation of the FIDO client. Since it is critical that we do not want to introduce a way to bypass the RP binding of a FIDO key, for any FIDO authenticators which will provide additional interface to support PKI, a concrete access control or firewall mechanism is required to make sure that the keys used by FIDO will not be accessible by any PKI-enabled applications.

The embedded PKI module will have a well-defined PKCS#11 interface acting as a bridge between FIDO Client and ASM. This will provide an abstraction layer between FIDO Client and the underlying cryptographic manipulations within authenticators. The PKCS interface can re-use some of the authenticator commands during create/generate/modify/delete of the cryptography objects or can implement its own methods. The PKCS#15 keystore interface within the ASM will assist key store/retrieval/ revoke operations with a different type of storage of FIDO authenticators (i.e., First-factor Bound, Second-factor Bound, First Factor Roaming and Second-factor Roaming authenticator).

3.1.2. FIDO uses PKI token

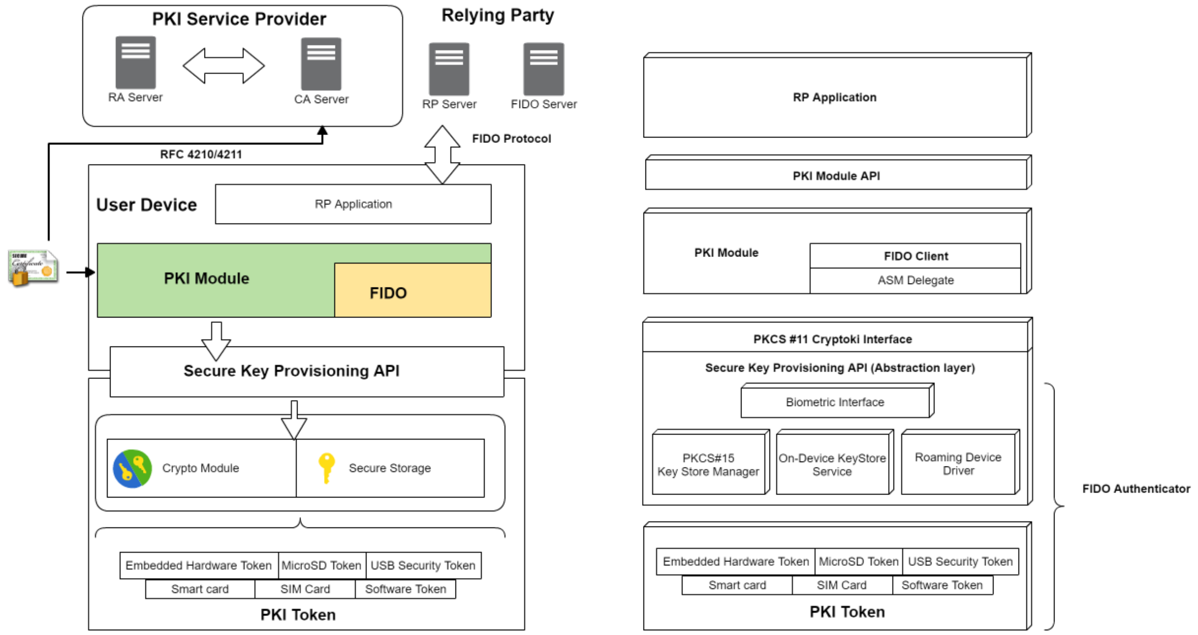


Figure 20. FIDO use PKI's Token

In a PKI system, a token is a "Security Token"[34] with the PKI module inside the token. There are some scenarios in which a service provider already has legacy PKI infrastructure. In this case, a RP Application could be highly coupled with the PKI module which could require extra effort when integrating with FIDO solutions.

The proposed guidance for this kind of integration is to have a FIDO Client and ASM delegation embedded into the PKI module. The underlying cryptographic operations are mostly supported by standard PKI interfaces. Therefore, a FIDO Client is acting as a message dispatcher when the RP Application triggers the PKI Module to conduct FIDO operations; the ASM delegate will leverage the existing standardized PKI interface to manipulate cryptography objects and bridge the operations with different authentication methods (e.g., biometrics, PIN methods).

3.2. Server side

Here are the suggested mechanisms for Class 1 and Class 2 on server side:

3.2.1. Class 1 (Shared authenticator)

In Class 1, FIDO UAF and PKI can share the client's authenticator to store their keys. FIDO and PKI keys are separated during the registration, authentication, and transaction process. The benefit of this solution is that just only one type of authenticator would be carried in a user device for satisfying FIDO-based and PKI-based applications at the same time.

3.2.2. Class 2 (Synchronized Registration Process)

In this Class, for the registration process we have three different approaches based on whether the user has an existing FIDO UAF key pair or PKI credential in advance. For authentication and transaction processes, we can use the key pair and protocols of either FIDO UAF or a PKI-based scheme on the requirement for the applications. For example, in most use cases FIDO can be used to authenticate the users, while PKI may be needed in some high risk transactions that require digital signature using the certificate issued by a Certificate Authority.

Note that for any approach in this class, the key pairs for FIDO and PKI are independent and will not be shared between each other.

3.2.2.1. Bootstrapping PKI Registration with FIDO

1. The user sends the initial authentication request to the FIDO UAF server.
2. The FIDO UAF server sends response to the authentication request to the FIDO client which triggers the local authentication process.
3. The authenticator requests the user to do the local authentication, and then unlocks the user's private key to sign the authentication response then pass it to the FIDO UAF server.
4. The FIDO UAF server verifies the authentication response and completes the authentication process.
5. The RP server (Web or App server) sends the request to the PKI Client to check whether the user has a valid certificate. If the user has no valid certificate, it then starts the registration process of PKI.
   5.1 Sends the initiate registration request to the PKI server.
   5.2 The PKI server sends the registration request to the PKI client.
   5.3 The PKI token asks the user to authenticate with their local password, PIN, biometric or other credentials, and to provide the signed pre-registration information which was verified by the RA (Registration Authority) securely.

5.4 Once the user is authenticated, the PKI token generates the user's PKI key-pair then returns the public key or PKCS#10 CSR (optional) to the PKI client.

5.5 If the PKI token returns the public key only, the PKI client will pack the unsigned certificate registration request and ask the PKI token to sign it using user's private key.

5.6 The signed certificate registration request, either returned from PKI token or packed by the PKI client, will be packed as the certificate issuing request with user's identity information and then send to PKI server to apply the PKI certificate.

5.7 The PKI server will verify the certificate issuing request with pre-registration information which was verified by the RA, and then sends the certification application to the CA to request the PKI certificate for the user.

5.8 The PKI server returns the Certificate Issuing Response to the PKI client with the certificate issued by the CA.

5.9 The PKI client verifies the received certificate then stores the certificate to local storage, or PKI token if the client supports certificate store.

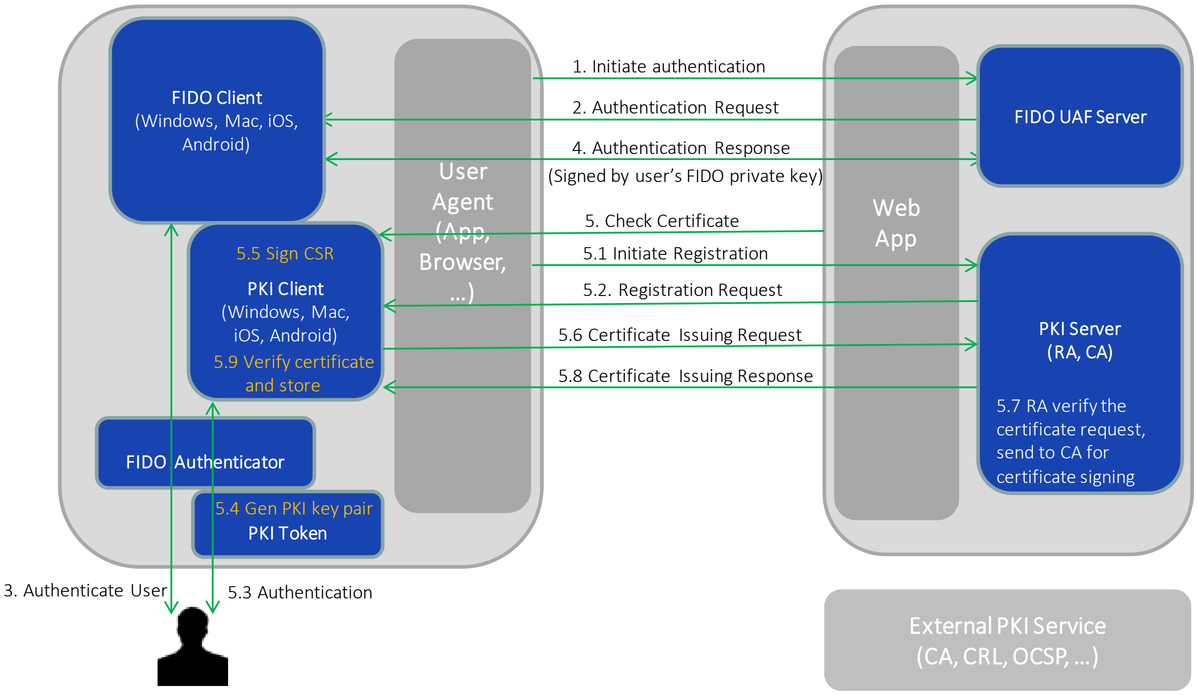

FIDO Client
(Windows, Mac, iOS, Android)
User Agent (App, Browser, ...)
1. Initiate authentication
2. Authentication Request
4. Authentication Response
(Signed by user's FIDO private key)
FIDO UAF Server
Web App
5. Check Certificate
5.5 Sign CSR
PKI Client
(Windows, Mac, iOS, Android)
5.9 Verify certificate and store
5.1 Initiate Registration
5.2. Registration Request
5.6 Certificate Issuing Request
5.8 Certificate Issuing Response
PKI Server
(RA, CA)
5.7 RA verify the certificate request, send to CA for certificate signing
FIDO Authenticator
5.4 Gen PKI key pair
PKI Token
3. Authenticate User
5.3 Authentication
External PKI Service
(CA, CRL, OCSP, ...)

Figure 21. Bootstrapping PKI registration with FIDO

3.2.2.2. Bootstrapping FIDO Registration with PKI

1. The user sends initial registration request to the FIDO UAF server.

2. The FIDO UAF server send response to the registration request to FIDO client.

3. The FIDO client calls the authenticator to authenticate user using local password, PIN, biometric or other credentials.

4. The FIDO authenticator generates the user's key-pair and signs the registration response.

   4.1 The client prompts the user to select the certificate.

   4.2 The user unlocks the private key associated with the selected certificate.

   4.3 The client signs the registration response with the unlocked private key, and attaches the signature and the certificate chain to the extension of the response.

5. The client sends the registration response to FIDO UAF server.

6. The FIDO UAF server verifies the status of the certificate to complete the FIDO UAF registration process.

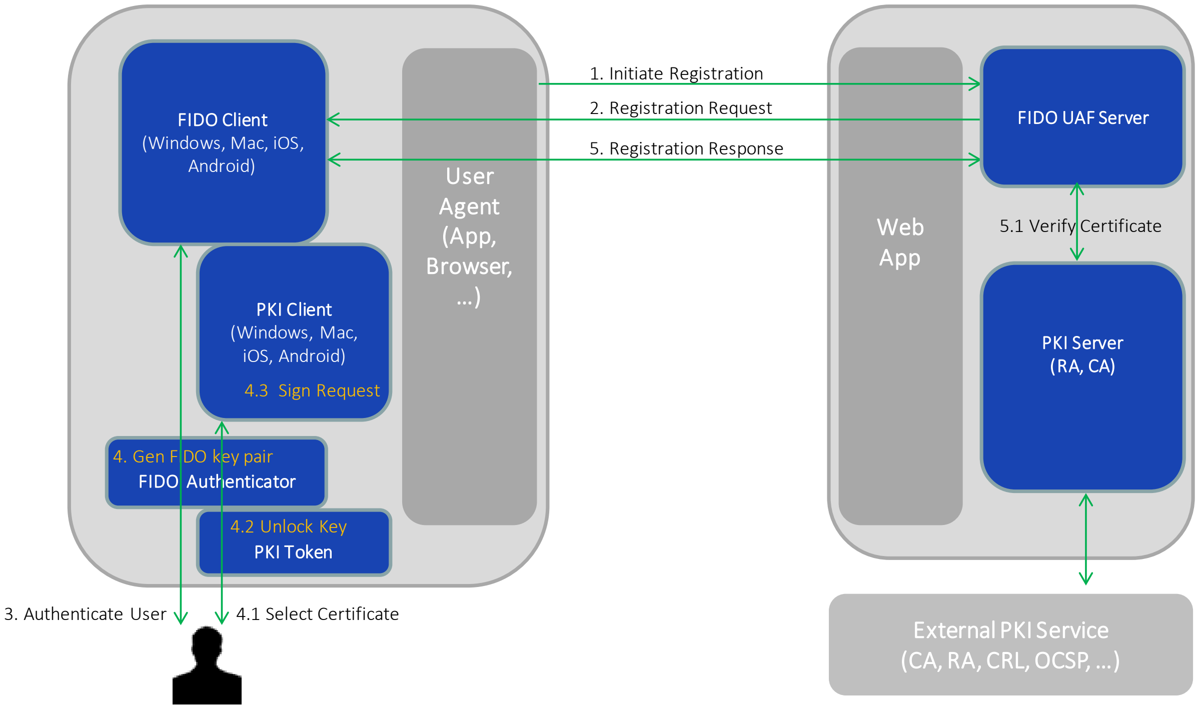


Figure 22. Bootstrapping FIDO registration with PKI

3.2.2.3. Combined Registration for FIDO and PKI

1. The user sends initial registration request to the FIDO UAF server.

2. The FIDO UAF server response the registration request to FIDO client.
3. The FIDO client calls the authenticator to authenticate the user using local password, PIN, biometric or other credentials.
4. The FIDO authenticator generates a user key-pair and signs the registration response.
5. The FIDO client sends the registration response to the FIDO UAF server to complete the FIDO registration process.
6. Once the FIDO registration succeeds, it starts the registration process for PKI:
   6.1 When user send initial request to the FIDO UAF server, user also sends the initial request to the PKI server.
   6.2 The PKI server sends the registration request to the PKI client.
   6.3 The PKI token asks the user to authenticate with their local password, PIN, biometric or other credentials, and to provide the signed pre-registration information which was verified by the RA securely.
   6.4 Once the user is authenticated, the PKI token will generate the user's PKI key-pair then return the public key or PKCS#10 CSR (optional) to the PKI client.
   6.5 If the PKI token return the public key only, the PKI client will pack the unsigned certificate registration request and ask the PKI token to sign it using user's private key.
   6.6 The signed certificate registration request, either returned from KI Token or packed by the PKI client, will be packed as a certificate issuing request with the user's identity information and then sent to the PKI server to apply the PKI certificate.
   6.7 The PKI server will verify the certificate issuing request with pre-registration information which was verified by the RA, and then sends the certification application to the CA (Certification Authority) to request the PKI certificate for the user.
   6.8 The PKI server returns the Certificate Issuing Response to the PKI client with the certificate issued by the CA.
   6.9 The PKI client verifies the received certificate then stores the certificate to local storage, or PKI token if it supports certificate store.

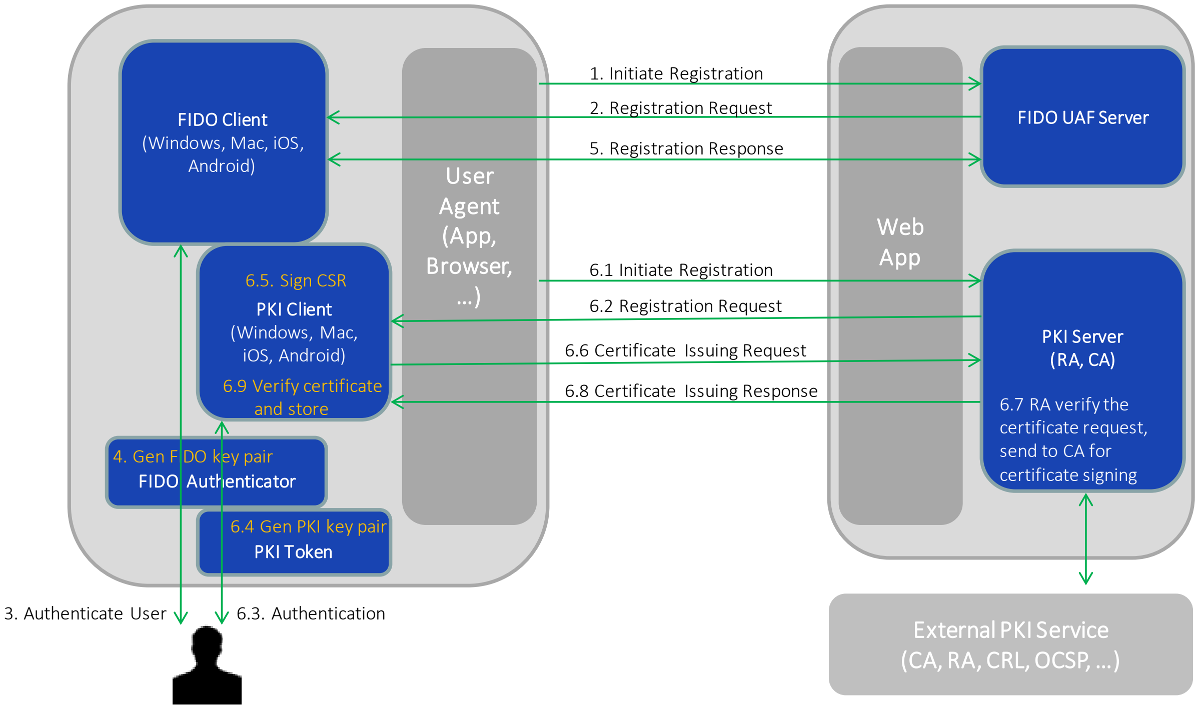


Figure 23. Combined Registration for FIDO and PKI

3.2.2.4. Revocation Process

For the approach of "Bootstrapping FIDO Credential with PKI" and "Combined Registration for FIDO and PKI", when the certificate is revoked it is recommended to deregister the FIDO credential. For the other approaches, if the user is not provided with the option to be registered with PKI and issued a certificate again then it is also recommended to deregister the FIDO credential as well.

1. When the user wants to revoke their certificate for some reason, the Revocation Request is sent to the PKI server.
2. The PKI server verifies the Revocation Request with the user's identity check using some out-of-band ways then sends the request to the CA to revoke user's certificate.
   2.1 The User Agent continues to process FIDO deregistration.
   2.2 The FIDO UAF server sends the deregistration request to the FIDO client.
   2.3 The FIDO client sends the command to the FIDO authenticator to delete the FIDO key-pair.
3. The PKI server returns the revocation result to the PKI client.
4. The PKI server sends the command to the PKI token to delete the user's private key.

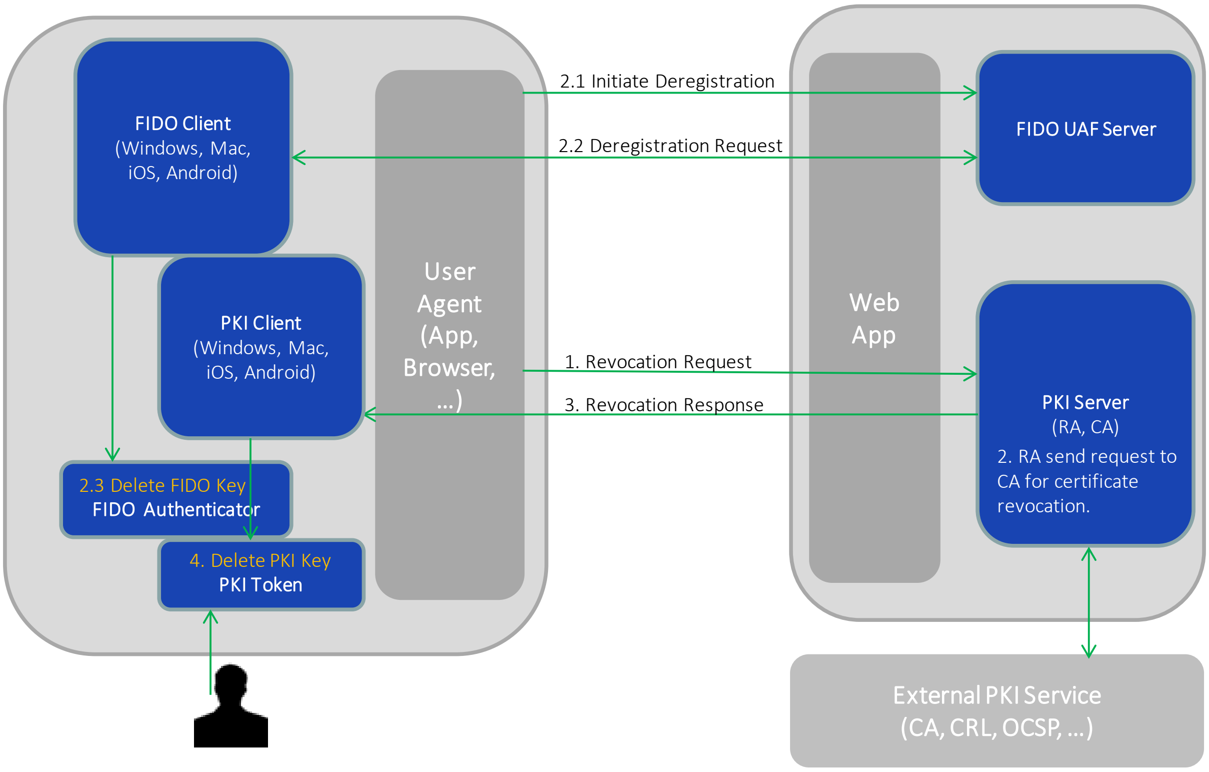


Figure 24. Revocation process in Class 2

4. Acknowledgements

- Andrew Shikiar, FIDO Alliance
- Anthony Nadalin, Microsoft
- Chung-Yi Lin. Chunghwa Telecom
- Eric Fan. National Taiwan University of Science and Technology, NTUST
- George Tang. Egis Technology Inc.
- John Fontana, Yubico
- Jonghyun Baek. Korea Internet and Security Agency, KISA
- Karen Chang. Taiwan Association of Information and Communication Standards, TAICS; Egis Technology Inc.; Asia PKI Consortium, APKIC
- Max Hata, FIDO Deployment at Scale WG Co-Chair
- Michael Magrath, VASCO Data Security
- Oliver Lien. Taiwan-CA Inc., TWCA
- Phoebe Ip. Macao Post and Telecommunications eSignTrust Certification Services,
- Robin Lin. Taiwan-CA Inc., TWCA
- Rolf Lindemann. Nok Nok Labs
- Salah Machani. RSA
- Thitikorn Trakoonsirisak. Electronic Transactions Development Agency, ETDA
- Vijay Kumar. eMudhra
- Wei-Chung Hwang. Industrial Technology Research Institute, ITRI

5. References

[1] China Electronic Signature Act, 28 August 2004, http://www.gov.cn/flfg/2005-06/27/content_9785.htm

[2] Barcode payment regulation, The People' Bank of China, 27 December 2017, http://www.pbc.gov.cn/goutongjiaoliu/113456/113469/3450002/index.html

[3] Citizen Online Identification Service, Ministry of Public Service, China, http://eid.cn/

[4] Hongkong Post e-Cert, https://www.hongkongpost.gov.hk/index.html

[5] Electronic Transactions Ordinance (Cap. 553), Hong Kong SAR, 7 January 2000, https://www.elegislation.gov.hk/hk/cap553

[6] The Smart Identity Card, Hong Kong Immigration Department, http://www.immd.gov.hk/eng/services/hkid/smartid.html

[7] Controller of Certifying Authorities, Ministry of Electronics and Information Technology, Government of India, http://www.cca.gov.in/cca/

[8] Information Technology Act, Ministry of Electronics and Information, Government of India, 9 June 2000, http://www.meity.gov.in/content/information-technology-act

[9] Aadhaar , Unique Identification Authority of India (UIDAI), Government of India, https://uidai.gov.in/

[10] Japan Government PKI, http://www.gpki.go.jp/

[11] Act on Electronic Signatures and Certificate Business, Japan, 31 May 2000, http://www.cas.go.jp/jp/seisaku/hourei/data/aescb.pdf

[12] Individual Number Card, Japan, https://www.kojinbango-card.go.jp/en/

[13] Digital Signature Act, Korea, 5 February 1999, http://www.moleg.go.kr/english/korLawEng?pstSeq=52667

[14] Macao Post and Telecommunications eSignTrust Certification Services, https://www.esigntrust.com/cn/index.php

[15] Electronic Documents and Signatures Law, Macao SAR, 8 August 2005, http://images.io.gov.mo/bo/i/2005/32/lei-5-2005.pdf

[16] Government Public Key Infrastructure, National Development Council, Taiwan, http://grca.nat.gov.tw/GRCAeng/index.html

[17] Financial Policy Management Authority, The Bankers Association, http://www.ba.org.tw/AboutUnion/CommitteeIntroduction?roleid=bd179fd9-4694-435e-ac0e-bd0d10227979

[18] Electronic Signature Act, Ministry of Economic Affairs, Taiwan, 14 November 2001, http://law.moj.gov.tw/Eng/LawClass/LawAll.aspx?PCode=J0080037

[19] Regulations Governing the Standards for Information System and Security Management of Electronic Payment Institutions, Financial Supervisory Commission, 28 December 2017, http://law.fsc.gov.tw/law/LawContentDetails.aspx?id=GL001541&KeyWordHL

[20] Taiwan Stock Exchange Corporation Directions for the Use of Digital Signatures by Securities Firms, Taiwan Stock Exchange, 19 April 2006, http://twse-regulation.twse.com.tw/ENG/EN/law/DAT0201.aspx?FLCODE=FL021988

[21] Citizen Digital Certificate, Ministry of Interior, Taiwan, http://moica.nat.gov.tw/

[22] Thailand National Root Certification Authority, http://www.nrca.go.th/

[23] Electronic. Transactions Act, 2 December 2001, https://www.bot.or.th/English/PaymentSystems/OversightOfEmoney/RelatedLaw/Documents/et_act_2544_Eng.pdf

[24] Trust Services and eID, Digital Single Market - European Commission, 23 July 2014, https://ec.europa.eu/digital-single-market/en/policies/trust-services-and-eidentification

[25] Korea Internet & Security Agency (KISA), http://www.kisa.or.kr/eng/main.jsp

[26] Chunghwa Telecom, http://www.cht.com.tw/en/

[27] Taiwan-CA Inc. (TWCA), https://www.twca.com.tw/Portal/english/coporate_profile/mission.html

[28] Macao Post and Telecommunications Bureau, http://www.ctt.gov.mo/en/

[29] Using Two-Factor Authentication Tools, BOCNET Corp., https://cbs.bocmacau.com/enterprise/en/securityInformation.html#link5

[30] Implementation Guideline for Safe Usage of Accredited Certificate using bio information in Smartphone, 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

[31] FIDO UAF Architectural Overview, FIDO Alliance, December 2014, https://fidoalliance.org/specifications/download/

[32] NIST Special Publication 800-157, Guidelines for Derived Personal Identity Verification (PIV) Credentials

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

[34] Security Token, https://en.wikipedia.org/wiki/Security_token