TTA Technical Report

기술보고서

TTAR-xx.xxxx

제정일: 2018년 4월 5일

아시아의 FIDO와 PKI
- 사례연구(기술보고서)

FIDO and PKI in Asia
- Case Study(Technical Report)

한국정보통신기술협회
Telecommunications Technology Association

기술보고서 초안 검토 위원회 개인정보보호/ID관리 블록체인 보안 프로젝트그룹(PG502)

기술보고서안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	기술보고서번호
기술보고서(과제) 제안	류하나	한국FIDO 산업포럼	차장	-	
기술보고서 초안 작성자	류하나	한국FIDO 산업포럼	차장	-	
	이기혁	한국FIDO 산업포럼	교수		
	홍동표	한국FIDO 산업포럼	분과장	-	
사무국 담당	박수정	TTA	책임		

본 기술보고서 발간 이전에 접수된 지식재산권 확약서 정보는 본 기술보고서의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 기술보고서와 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 기술보고서의 목적

이 기술보고서는 아시아 국가에서 FIDO와 PKI를 통합하기 위한 현재 또는 계획된 사례를 제공하고, 해당 사례를 통해 FIDO 기술을 통한 PKI 체계의 변화에 대한 정보 제공을 목적으로 한다.

2 주요 내용 요약

아시아에서 PKI(Public Key Infrastructure)는 금융, 의료 및 정부를 포함하여 규제가 심한 산업 분야에서 신뢰할 수 있는 인프라를 확보하는 데 매우 중요한 역할을 하고 있다. 기존의 PKI 시스템을 기반으로 한 FIDO 표준의 가속화로 FIDO 표준을 도입함으로서 조직은 기존의 PKI 인프라를 활용할 수 있게 되고, 사용자에게 더 좋은 PKI 애플리케이션을 제공하기 위해 작성되었다. 이 기술보고서는 FIDO 및 아시아 PKI 컨소시엄(Asia PKI Consortium, APKIC) 멤버들이 실제 활용하는 PKI 기술 그리고 FIDO 기술을 적용한 PKI 기술, 두 가지 항목으로 구분하였다.

1. 아시아 국가 내 PKI 와 관련된 기술 개요 소개
   가. 한국, 대만, 태국, 마카오, 인도에서의 PKI를 통한 인증 및 거래 기술 사용
   나. 각 국가별 금융, 공공 또는 신원확인 체계 적용 현황

2. FIDO 기술과 PKI 기술의 접목을 통한 PKI 체계의 확장 모델 소개
   가. FIDO 기술 및 스마트폰 내 안전한 보호 영역과 결합한 PKI 적용
   나. FIDO 등록과 인증서 발급, 사용에 따른 인증 체계분석

3 인용 기술보고서와의 비교

Asia PKI Consortium(2018), FIDO Alliance and Asia PKI Consortium White Paper: FIDO UAF and PKI in Asia - Case Study and Recommendations

3.1 인용 기술보고서와의 관련성

이 기술보고서는 아시아 PKI 컨소시엄의 'FIDO Alliance and Asia PKI Consortium White Paper: FIDO UAF and PKI in Asia - Case Study and Recommendations' 기반으로 작성되었음

3.2 인용 표준과 본 기술보고서의 비교표

단체표준안	참조표준	비고
6. 아시아에서의 PKI현황	제1장	동일 및 일부 기술 내용 추가
7. FIDO와 PKI 사례 연구	제2장	동일 및 일부 기술 내용 추가

Preface

1 Purpose

The standard provides the current or planned cases to integrate FIDO and PKI in Asian countries. The purpose of this case study is to provide information on the change of PKI system through FIDO technology

2 Summary

The standard is designed to provide 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. This technical report is divided into two categories: PKI technology that FIDO and Asia PKI Consortium (APKIC) members use, and PKI technology that uses FIDO technology:

1. Introduction of PKI-related technology outline in Asian countries
   a. Using PKI authentication and transaction technology in Korea, Taiwan, Thailand, Macao and India
   b. Application of financial, public or identity verification system by country

2. Introduction of extended model of PKI system by combining FIDO technology and PKI technology
   a. PKI combined with FIDO technology and secure area of protection on smartphone
   b. FIDO registration, certificate issuance, analysis of authentication system according to use

3 Relationship to Reference Standards

The technical report is based on 'FIDO Alliance and Asia PKI Consortium White Paper: FIDO UAF and PKI in Asia - Case Study and Recommendations' written by Asia PKI Consortium.

목 차

아시아의 FIDO와 PKI -사례연구
(FIDO and PKI in Asia - Case Study)

1 적용 범위

이 기술보고서는 아시아 국가에서 FIDO와 PKI를 통합하기 위한 현재 또는 계획된 사례를 제공하고, FIDO 및 아시아 PKI 컨소시엄(Asia PKI Consortium, APKIC) 멤버들이 실제 활용하는 FIDO 기술표준 또는 FIDO 기술을 적용한 PKI 체계의 기술분석을 제공한다.

2 인용 표준

- 해당사항 없음

3 용어 정의

- 해당사항 없음

4 약어

FIDO	Fast IDentity Online
PKI	Public Key Infrastructure
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol
CTAP	Client to Authenticator Protocol
NPKI	National Public Key Infrastructure
GPI	Government Public Key Infrastructure
MPKI	Military Public Key Infrastructure

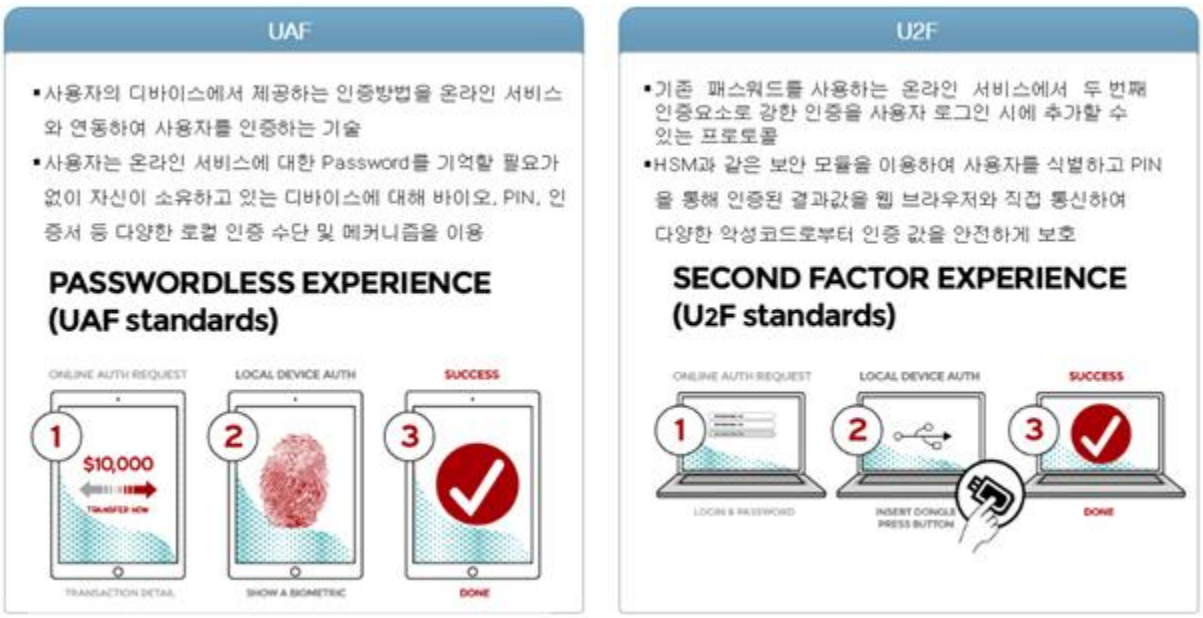
5 개요

한국, 중국, 인도, 대만, 태국, 홍콩, 마카오와 같은 많은 아시아 국가/지역에서는 국가적 PKI/eID 인프라를 법률로 제정했다. APKIC는 해당 지역의 PKI 간의 상호 운용성을 높이고, 해당 지역의 PKI를 활용하여 전자 상거래를 활성하기 위한 해당 지역의 금융 및 정부 부문을 대표한다. 아시아 이외에 전자식별 및 트러스트(Trust) 서비스에 관한 유럽 연합(EU)의 910/2014 규정은 2016년 7월 1일부터 시행되었다. eIDAS는 전자서명, 전자거래, 관련 기관 및 해당 임베디드 프로세스를 통해 사용자가 전자거래를 수행할 수 있는 안전한 방법을 제공한다. 본 표준은 아시아에서의 PKI 개발된 내용을 조사하여 작성된 자료이다.

5.1 FIDO정의

FIDO(Fast Identity Online) Alliance는 온라인 환경에서 생체인식기술을 활용한 인증방식에 대한 기술표준을 정하기 위해 2012년 7월 설립된 협의회이다. 회원사로는 아마존, 구글, 삼성전자, ARM, 마이크로소프트 등이 가입되어 있으며, 2014년 12월 국제 인증기술 표준인 FIDO 1.0을 공개하였다.

5.1.1 FIDO 1.0 연계표준

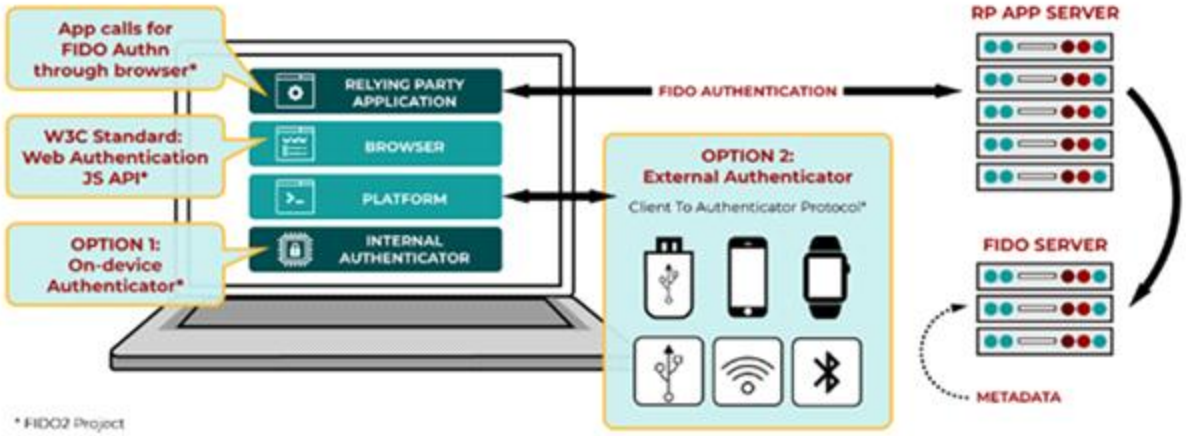


(그림 5-1) FIDO 인증장치 규격 유형 (출처: FIDO Alliance)

5.1.2 FIDO 2 연계표준

FIDO Alliance 에서는 기존의 FIDO1.0을 기반으로 하는 생체인증 국제 표준은 사용자의 스마트폰을 중심으로 모바일 생태계 내 호환에 중점을 맞추었으나, 기존 PC환경 체계와 순수한 웹브라우저 환경에서의 생체인증 확장을 위해 신규 표준을 제시함. 이에 다양한 웹브라우저(크롬·엣지·파이어폭스) 제공사에서는 신규 FIDO 표준을 구현하기 시작했고, 윈도, 맥, 리눅스 등 다양한 OS 진영에서도 적용을 시작하고 있음.

특히 FIDO Alliance 에서는 신규 표준 출시시, 기존 FIDO1.0 규격을 모두 업그레이드 해야 할 것이라는 고객사, 솔루션 벤더사 등의 오해를 불식시키기 위하여, 신규 표준은 전혀 다른 스펙이라는 부분의 강조를 위해, ‘FIDO2.0’ 이 아닌 ‘FIDO2’ 로 명명하였다.
이를 통해, FIDO2 표준은 FIDO1.0 표준의 업그레이드가 아닌 새로운 시장으로 진입 의지를 표명하였다.



(그림 5-2) FIDO2 기본 사상 (출처: FIDO Alliance)

FIDO2 는 크게 W3C의 WebAuthn과 외부인증장치인 CTAP (Client to Authenticator Protocol)으로 나누어진다.

- WebAuthn 은 온라인 서비스상에서 FIDO인증을 사용할 수 있도록 기존의 스마트폰의 앱 기반이 아닌 브라우저에 내장할 수 있는 표준 API를 정의.
- CTAP 은 스마트워치, 스마트폰, USB 형태와 같은 디바이스를 통해, WebAuthn을 연동하여, PC내 응용 프로그램 또는 웹서비스의 인증을 연동.
- 기존 FIDO1.0의 인증장치 유형이 UAF와 U2F방식이었으나, FIDO2의 출현에 따라 FIDO는 UAF, U2F, WebAuthn, CTAP으로 인증장치 유형의 범위를 확장함.

5.2 PKI 정의

PKI(Public Key Infrastructure)란 전자금융 거래의 비밀을 보장하면서도 거래 당사자의 신분을 확인시켜주는 보안기술을 말하며 일반적으로는 공개키 기반 구조라 칭한다. 즉 공개키를 효과적으로 관리하기 위해 사용되는 모든 요소들을 포함한다. 공개키 암호화는 기밀성, 인증, 무결성, 부인방지의 기능을 제공하는 가장 일반적으로 사용되는 암호화 방법이라 할 수 있다. 따라서 공개키 암호화가 사용되는 모든 사용자, 클라이언트, 서버 마다 각각의 개인키-공개키 쌍이 필요하다. PKI는 이런 개인키-공개키의 생성 및 인증 과정을 안전하고 효과적으로 관리 할 수 있도록 지원한다.

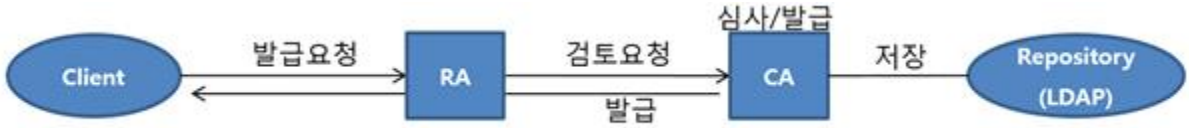
5.2.1 PKI 기반 공인인증서 구성

CA(Certificate Authority):
인증서 발급 주체(Issuer) 이며, 인증기관 및 이를 신뢰해주는 중계CA, 최상위 CA등으로 구분되며, 인증서 발급/폐기/재발급/보관 등의 역할을 진행한다.
인증서 유효성의 검증을 위해서는 기본적으로 LDAP내 CRL(Certificate Revocation List)를 배포하며, 실시간 유효성 검증을 지원하기 위해 OCSP(Online Certificate Status Protocol)을 지원한다.

RA(Regional Authority):
CA업무를 대행하는 기관으로써, 인증서의 발급을 위한 사용자의 신원 확인 과정을 수행하며, 참조/인가코드를 사용자에게 부여한다.
사용자 신원확인이 가능한 인프라를 갖추고 신뢰성을 담보할 수 있는 은행, 증권사 등에 해당한다.

LDAP(Light Data Access Protocol):
인증서의 유효성 확인을 할 수 있도록 CRL을 배포하는 저장소이며, CA에서 사용자의 인증서 및 CRL 목록을 배포한다.
다양한 서비스에서의 많은 조회건수를 처리하기 위해, 조회에 최적화된 LDAP을 기본으로 한다.

OCSP(Online Certificate Status Protocol):
CRL 유효성 검증 방식의 시간 간격에 대한 취약점을 개선하고자, 실시간 형태의 인증서 상태 검증을 제공하는 서비스 프로토콜을 의미한다.



(그림 5-3) PKI 인증서 발급을 위한 신원 확인 절차

5.2.2 공인인증서 체계내 전자서명 및 검증 흐름

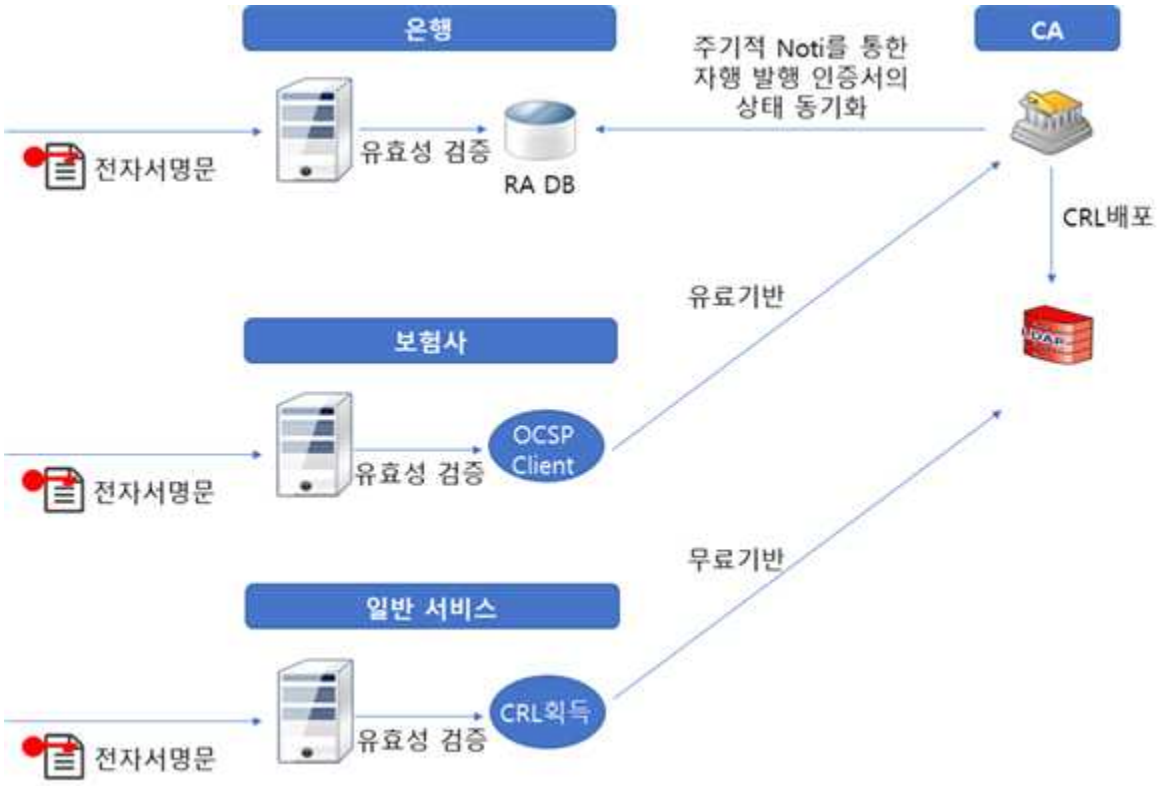
전자서명을 수행하는 사용자의 적합성 확인을 위해 PKCS#5 규격으로 보호되는 인증서에 대한 확인 절차(비밀번호 입력)를 통해 전자서명문 생성. 이후 이를 전송받은 서비스에서는 해당 서명문이 정상적으로 서명되었는지 검증하는 절차를 수행한 후, CA측에 해당 인증서의 유효성을 검증하게 된다.
서명문 검증은 X.509 포맷, 전자서명의 무결성 뿐만 아니라, 서비스를 제공하는 제공사측에서 수용할 수 있는 인증서인지를 판단하는 OID 정책의 검증까지도 포함되고 있다.
서명문 검증부분은 일반적으로 PKCS#7 기반의 전자서명문을 검증하는 체계로 구성되어 있으며, 주식거래와 같은 특수 시장에서는 PKCS#1 형태의 전자서명문을 사용하고 있다.

(그림 5-4) 전자서명 검증 체계

5.2.3 공인인증서의 유효성 검증 체계 흐름

인증서의 유효성을 검증하는 방식은 기본적으로 CRL 및 OCSP 방식이 존재하며, RA를 직접적으로 운영하는 금융사 또는 기관에서는 인증 발급내역에 대한 상태를 RA DB내 동기화하여 직접적인 조회가 가능하다.

유효성 방식별 적용은 RA의 보유 유무, 서비스의 중요성에 따라 아래와 같이 나누어 볼 수 있다.



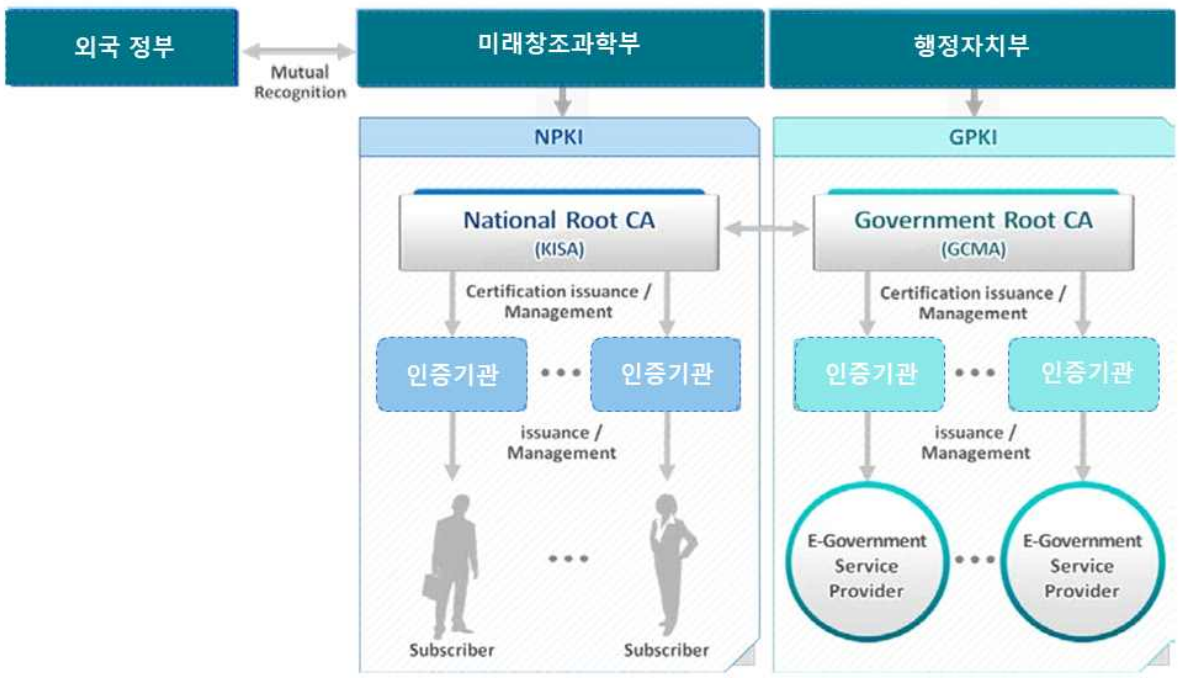
(그림 5-5) 서비스별 인증서 유효성 검증 체계

6. 아시아에서의 PKI 현황

한국, 중국, 인도, 대만, 태국, 홍콩, 마카오와 같은 많은 아시아 국가/지역에서는 국가적 PKI/eID 인프라를 법률로 제정했다. APKIC는 해당 지역의 PKI 간의 상호 운용성을 높이고, 해당 지역의 PKI를 활용하여 전자 상거래를 활성하기 위한 해당 지역의 금융 및 정부 부문을 대표한다.
아시아 이외에 전자식별 및 트러스트(Trust) 서비스에 관한 유럽 연합(EU)의 910/2014 규정은 2016년 7월 1일부터 시행 되었다. eIDAS는 전자서명, 전자거래, 관련 기관 및 해당 임베디드 프로세스를 통해 사용자가 전자거래를 수행할 수 있는 안전한 방법을 제공한다.

6.1 한국

한국은 두가지 개념의 PKI가 있다. 하나는 개인과 회사를 위한 것이고, 다른 하나는 정부 공무원을 위한 것이다. 국가 PKI(National PKI, NPKI)는 1999년 '전자서명법' 하에 구축되었다.

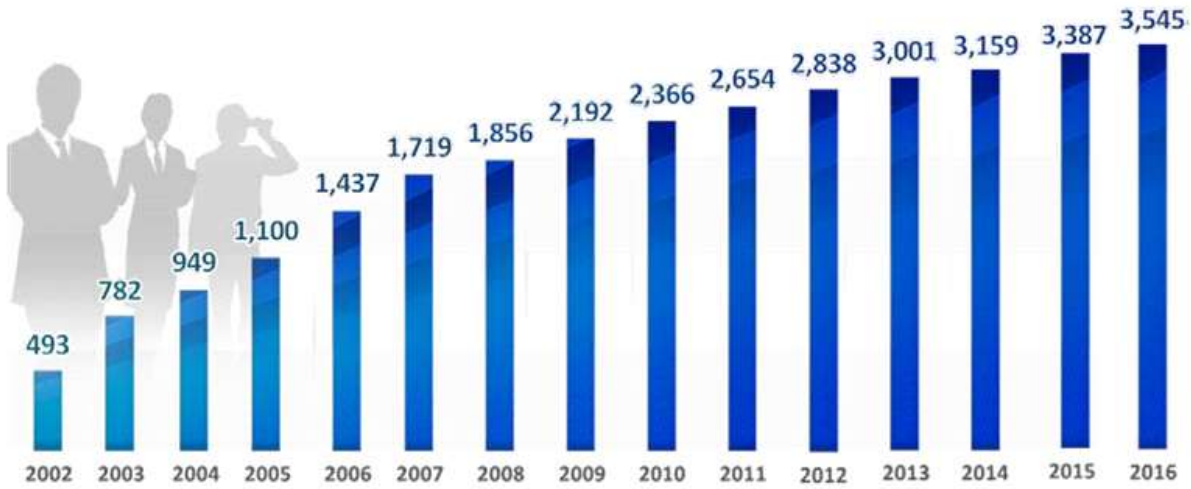


(그림 6-1) 국내 공인 PKI 모델 (출처: APKIC)

6.1.1 NPKI 체계

NPKI의 관할 기관은 과학기술정보통신부(이하 과기정통부)이다. 한국인터넷진흥원(KISA)은 과기정통부에서 최상위 인증기관의 역할을 수행한다. NPKI 인증서는 인정된 인증기관으로부터 개인 및 회사에게 발급되며 가입자는 인증서를 사용하여, 온라인 정부 서비스에 대한 인증을 받을 수 있다.

2016 NPKI로 승인된 인증기관에서 발급한 인증서 수가 3545만개이며, NPKI 인증서는 인터넷 뱅킹, 온라인 주식 거래, 온라인 쇼핑 및 전자 정부 (G2C) 서비스에 널리 사용된다.



(그림 6-2) 국내 NPKI 인증서 발급 현황 (출처: APKIC)

NPKI 인증서는 전자서명을 통한 온라인 인증 및 거래에 대한 전자서명 두 가지의 용도 외 본인확인이라는 신원확인 기능을 지원한다.
신원확인 기능은, 해쉬처리된 주민번호를 인증서 내부에 저장하여, 전자서명 주체와 주민번호 소유자의 일치성을 보장하고 이를 기반으로 사용자 식별이 필요한 서비스에 활용하고 있다.

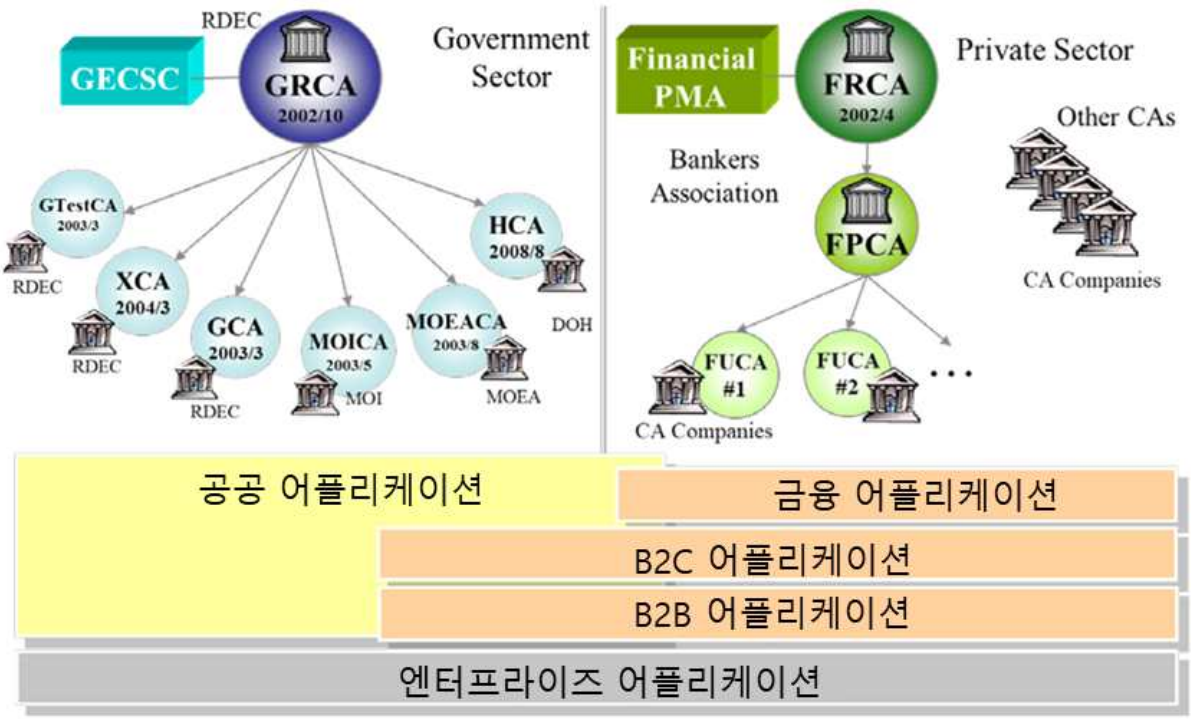
6.1.2 GPKI, MPKI 체계

정부PKI는 2001년 '전자정부법'에 따라 설립되었으며, 이 분야의 관할 기관은 행정안전부(이하 행안부)이며, 공무원에게만 인증서를 발급한다. 그들은 민간 영역에서 GPKI 인증서를 사용한다. NPKI와 GPKI간의 상호 운용성을 위해 두 분야에는 인증서신뢰목록(CTL, Certificate Trust List)이 별도로 발급된다.

국방전용 인증서인 MPKI 체계는 국방 폐쇄망 내 운영되는 형태의 인증서 체계로써, 범용적인 인증서가 아닌 특수목적용 사설인증서 체계로 보는 것이 적합하며, 높은 보안 수준의 유지를 위해서 보안토큰 내 인증서를 저장하여 사용한다.

6.2 대만

대만은 2001년 11월 14일에 전자서명법 (Electronic Signature Act)을 제정했다. 이 법안은 전자 기록 및 전자 서명의 법적 지위 및 사용을 규율한다. 그 이후 정부 및 민간 부문은, 특히 전자 정부 및 금융 부문에서 PKI 시스템을 개발하는데 전념 해왔다.



(그림 6-3) 대만 PKI 현황 (출처: APKIC)

6.2.1. 정부 PKI

1997년 최초의 정부 인증기관(GCA)가 인증서를 발급한 이래로, 대만의 정부 공개키 인프라인 GPKI는 각기 다른 부처에 의해 설립되어 여러 개의 인증기관으로 구성된 계층 구조의 PKI로 발전했다. [그림 6]은 대만 GPKI의 계층 구조의 인증기관을 보여준다. 광범위한 PKI 기술 채택은 대만 전자 정부의 정보보안을 향상시켰을 뿐 아니라 더 큰 효율성 및 탄소 저감 효과를 준다.

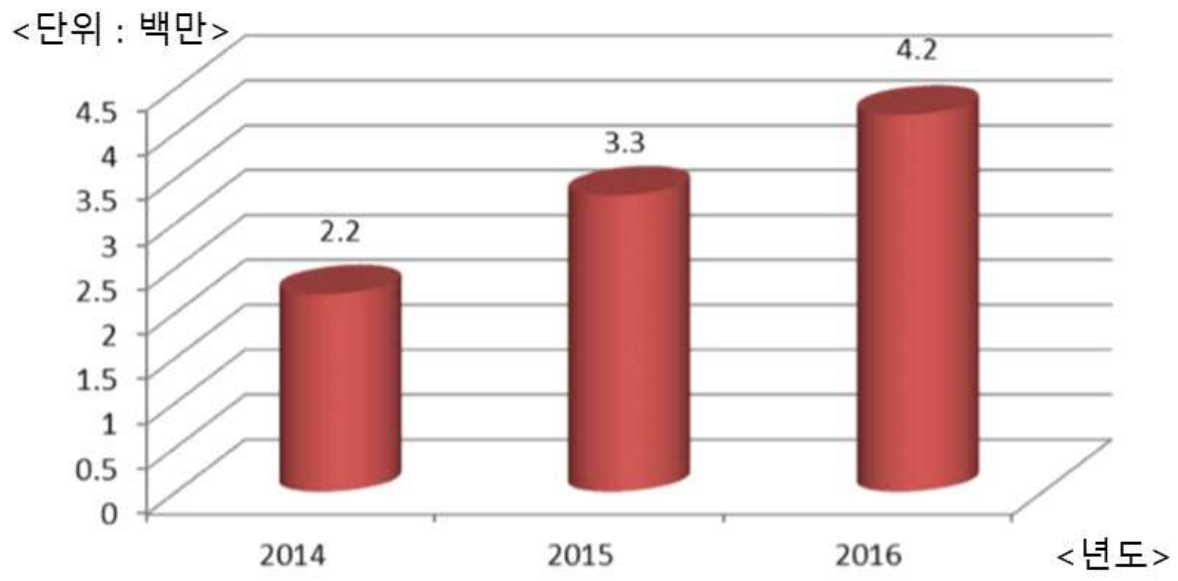
대만의 인증기관(GPKI, GRCA, GCA, MOEACA, MOICA, XCA, GTestCA) 중에서는 Chunghwa Telecom에 아웃소싱 되었다. 전부 Chunghwa Telecom이 개발한 HiPKI Certificate Management Suite를 사용하여 설치된다.
GPKI에서 발행한 스마트카드는 투팩터 인증을 지원하며, 기존의 단일인증과 ID/PW 로그인을 대체 할 수 있다. 또한 전자서명 및 암호화 메커니즘은 무결성, 부인 방지 및 온라인 거래의 기밀성을 보호함으로써 정보 보안을 강화시킨다. 종이 문서에 서명하는 수동 프로세스를 전자 서명 프로세스로 대체함으로써, 효율성이 개선되고 종이 사용량이 감소

하였다. 이 제품이 발행한 스마트카드의 수는 이미 4 백만이 넘는다.

6.2.2. 금융 PKI

대만에서는 금융 서비스(사이버 보안, 은행 및 보험 응용 프로그램 포함)가 민간 영역에서 가장 중요한 역할을 한다. 대만인증기관(TWCA, Taiwan Certificate Authority Corporation)은 금융 시장에서 가장 큰 비중을 차지한다.
TWCA은 처음에는 보안 및 은행 업무를 통해 PKI의 기초를 마련하고, 보험, 전자투표, 전자세금 등 더 많은 용도를 개발했다. 일부 정부 서비스도 전자세금을 포함한 사설인증서를 채택하기 시작했다.
많은 서비스 제공 업체는 새로운 사용자를 온라인으로 식별하고자 하지만 방법은 제한적이다.

현재 모든 사용자는 지사에 직접 개인 인증서를 신청해야 한다. 발급된 인증서는 온라인 서비스 공급자가 새로운 사용자를 식별하는데 필수적이다.
또한 TWCA는 전자ID, 국민 건강 카드, 직불 카드 등 다중 지원하는 온라인 인증 솔루션을 기업에 제공한다. 이 솔루션을 통해 금융 기관은 온라인 상에서 새로운 사용자를 훨씬 쉽고 명확하게 식별할 수 있는 몇 가지 요소를 활용할 수 있다. 2016년 TWCA은 민간 부문에서 420만 개의 인증서를 발급했다.



(그림 6-4) 대만 PKI 인증서 발급 현황 (출처: APKIC)

6.3 태국

디지털 시대를 맞이하는 것은 세계적 추세에 따라, 글로벌 경제는 기술적인 진보와 온라인 플랫폼의 사용 증가로 도래되고 있음이 분명하다. 온라인 활동의 증가, 디지털 인프라의 강력한 정부 지원 및 개선으로 인해 태국은 모바일 장치의 광범위한 사용은 물론 전자 정부 서비스, 전자 상거래 시장 및 지불시스템의 분명한 성장하고 있다.
태국의 정부 행정부서(Department of Provincial Administration, DoPA)는 신원을 증명하는 공식 문서인 태국인 신분증을 발급한다. 신분증은 카드 소지자에 대한 기본정보를 표시하는 것 외에도 암호화된 칩에 개인정보를 전자 형식으로 저장한다. 신분증은 공공 서비스 이용, 사업 설립 및 은행 계좌 개설과 같은 정부 및 기업 거래를 수행하는데 널리 사용된다.
사용자가 모바일 장치를 통해 편리하게 쇼핑할 수 있기 때문에 금융 거래를 수행해야하는 요구가 급격히 증가했다. 그러나 사용자 편의는 적절한 보안 및 인증의 균형을 이뤄야 한다. 특정 거래는 PKI 기술을 기반한 전자서명이 필요하다. 따라서 사용자가 모바일 기기로 안전하게 거래를 하기 위한 인증을 할 필요가 있다.
더 나은 편의를 위해 공공 및 민간 부문은 두 가지 목적을 모두 달성할 수 있는 최상의 기술을 찾고 있다. FIDO는 편리하고 안전한 인증을 제공하므로, 이러한 요구사항을 잠재적으로 해결할 수 있는 기술 중 하나이다.
그러나 특정 거래는 PKI 기술을 기반으로 하는 법적 구속력이 있는 법적인 전자서명이 필요하다. 휴대전화를 인증 및 전자서명 용도로 사용할 수 있다면 인터넷 거래가 훨씬 편리하다.

6.4 마카오

마카오 최초이자 현재, 특별행정구(Macao Special Administrative Region, MSAR) 가 인정한 유일한 인증 기관(CA)은 CTT eSignTrust Certificaion Services(eSignTrust)이다.
CTT는 마카오 우편통신국을 의미하며 (구, 마카오 우체국) 전자서명법(법령 No. 5/2005)에 의거하여 eSignTrust를 운영하고 있다.

6.4.1 eSignTrust 체계

eSignTrust는 MSAR의 전자문서 및 서명법(Electronic Documents and Signatures Law, EDS Law) No 5/2005 에 따라 마카오 우편 통신국인 CTT가 관리한다. 전자문서 및 서명법에 따라 다음과 같은 유형의 서명 및 인증이 정의된다.

AES(Advanced Electronic Signature)는 서명자와 고유하게 연결되어 있으며, 식별할 수 있고 자신이 관리 할 수 있는 방법을 사용하여 만들어지는 전자서명이다. 데이터의 작은 변경이 감지될 수 있는 방식으로 관련된 데이터에 연결된다. EDS에 따르면 AES와 서명한 전자 문서는 법적 효력을 가지며, 일반적인 법적 효력을 가지며, 일반적인 법적 규칙

과 관련 당사자의 합의에 따라 평가된다.

QES(Qualified Electronic Signature)는 공인인증서를 기반으로 한 고급스런 전자서명이다. EDS에 따르면, 공인 전자서명으로 서명 되어 서면 진술로 표현될 수 있는 전자 문서는 서명자의 귀속 선언에 대한 충분한 증거를 가진다.

ES(Electronic Signature)는 다른 전자 데이터에 첨부되거나 논리적으로 관련되며, 인증에 사용되는 전자 형식의 데이터이다. EDS법은 전자서명에 대한 법적 지원을 제공한다.

eSignTrust가 발행한 공인인증서는 개인 또는 전자적인 식별에 대한 인증서 보유자의 신원을 매우 높은 수준으로 보증한다. 해당키 쌍이 생성되어 SSCD(Secure Signature-Creation Device)에 포함된다. eSignTrust 공인인증서의 주요 용도는 QES를 생성하는 것이다. eSignTrust 공인인증서의 또 다른 용도는 인터넷 뱅킹에 의한 추가 인증 요소를 제공하는 것이다.
eSignTrust 인증기관은 개인, 조직 사용자 및 정부 기관에 고유한 신뢰성의 3가지 수준에서 디지털인증서를 발급한다. 인증서의 신뢰성은 가입자의 신원 확인 절차 및 eSignTrust가 등록 신청서에서 요청자가 제출한 데이터를 확인하기 위해 사용하는 노력에 따라 달라진다. 보안 수준의 강도와 복잡성이 높을수록, 높은 수준의 신뢰성이 달성되고 할당된다.

6.4.2 SignCloud 체계

eSignTrust는 eSignCloud 서비스를 출시하여 정부 부처, 비즈니스 조직 및 개인 사용자를 위해 실명 인증을 제공 할 수 있는 안전하고 신뢰할 수 있으며 사용자 친화적인 온라인 서명 도구를 제공한다. eSignCloud 서비스를 통해 사용자는 보안, 편의 및 법적 효력과 언제 어디서나 휴대 기기에서 전자문서에 서명 할 수 있다. "eSignCloud"는 AES 기반 서명 서비스이다. 온라인 응용 프로그램을 쉽게 통합 할 수 있도록 설계되었으므로 서명자의 신원 및 더 높은 법적 가치에 대한 실명 인증을 가능하게 하는 eSignable 웹 응용 프로그램으로 업그레이드 할 수 있다.

eSignCloud 서비스의 향상된 보안 및 편의성은 온라인 서비스 및 거래와 관련하여 대중의 신뢰를 높이는 데 도움이 된다.
eSignCloud 서비스는 사용자가 AES 인증서를 사용하여 계정을 만들 것을 요구하며 무료 eSignTrust MOTP(모바일 일회성 패스워드) 모바일 응용 프로그램과 함께 사용하여 보다 강력한 보호를 위한 2 단계 인증을 가능하게 한다. eSignCloud 서비스를 더욱 향상시키기 위해 eSignTrust는 다음과 같은 측면을 고려한다.

■ 서명 규칙 및 정책을 위한 포괄적인 모델
■ 인증 메커니즘 (지문, NFC, 스마트 ID 카드 등) 향상

■ 모든 서명 프로파일 지원
■ QES- 기반 eSignCloud
■ 국가 간 법적 승인 및 원격 인증 등록 프로세스
■ 전자식별, 전자 인증, 전자 서명 및 관련 서비스를 위한 믿을만한 서비스 구축

6.5 인도

인도의 전자 신원 확인 및 인증 서비스는 지난 15년 동안 성숙해 왔다. 최근 몇년 동안 정부는 종이 없는 서비스, 현금 없는 서비스, 존재하지 않는 서비스에 더 많은 노력을 기울였으며 정책과 혁신을 장려하고 있다.
전자 기록 및 전자 서명에 대한 법률은 2000년 인도에서 통과 되었고, 이는 IT 혁명에 있어 법적 지원을 제공했다. 이는 유엔 국경 간 전자 무역 촉진 프로그램의 위임 사항이기도 하다. 전자 인증의 조기 채택은 인도의 수입 및 수출 시스템을 위해 시작되었다.
전자 기록은 초기 움직임 이었지만 디지털/전자서명은 2004~5년에 눈에 띄었고 인도의 회사 법률 사무소에서는 전자 문서 처리를 도입했다. 2006~7년부터 더 많은 인구로 디지털 채택 서비스는 수입 증대를 가져왔다. 결국 전자 인증은 eProcurement 시스템, 철도 예약 에이전트, GST(Goods and Services Tax) 파일링 시스템, 정부 대 시민 서비스 등과 같은 대규모 구현을 채택했다.

6.5.1 AadHaar 체계

2011-12년 인도는 'Aadhaar'라는 최신 IDs(Identity system) 시스템을 도입했다. 이는 인구 통계 및 생체 인식 정보를 등록한 후 12 자리 숫자의 고유 번호로 인도의 모든 거주자에게 부여되는 독특한 카드 없는 신원입니다. 이것은 대규모 수용을 허용하는 매우 안전하고 구조화 된 시스템입니다. 현재 인도에서 11 억 7 천만 명이 이 프로그램에 참여하고 있다.(전체 인구의 95 % 이상)

Aadhaar의 독특한 점은 카드가 없는 행동이다. Aadhaar의 원본도 전자 방식으로 발급되며 (PKI 기반 디지털 서명 PDF) 모든 인증 시스템에서 직접 사용할 수 있다. 다른 면에서, 정부, 은행 및 기타 규제 기관은 Aadhaar와의 직접적인 온라인 검증을 위해 안전한 연결성을 확보 할 수 있다. 이 온라인 서비스는 PKI 소스-암호화로 보호되고 변조 방지 트랜잭션 모델로 서명된다. 이 서버를 사용하여 사용자는 12 자리수의 Aadhaar plus 인증 요소를 입력하여 인증 할 수 있다.
2015 년 인도는 정보 기술 법 (Information Technology Act)을 개정하여 세계 최대 전자 서명 (eSign) 프로그램을 시작했다. 이 전자 서명은 Aadhaar 시스템에 의해 지원되며 사용자가 즉시 서명 할 수 있다. 이로써 온라인 양식으로 식별, 인증 및 서명 프로세스에 PKI를 쉽게 채택 할 수 있는 많은 플랫폼이 용이하게 되었다. 오늘날, 은행 및 정부 시스템은 eSign을 사용하고 종이 없는 서비스를 지원한다. eSign은 널리 채택되어 현재 2,000만 명의 사용자를 보유하고 있으며 이는 국가 인구의 거의 2 %에 해당한다. 또한

컴퓨터 및 모바일 장치를 통해 하루에 20 만 건 이상의 트랜잭션을 처리 할 수 있다.

6.5.1. 애플리케이션

인도에서는 온라인 시스템이 날로 증가하고 있다.
1. 은행 및 금융 웹 사이트 응용 프로그램
2. 전자 상거래 웹 사이트 / 응용 프로그램
3. 세금 신고 웹 사이트
4. 기업 또는 소매 고객 로그인 웹 사이트 / 응용 프로그램
5. 정부와 시민 서비스
6. E - 웹 사이트 제공
7. 엔터테인먼트 / 영화 티켓
8. 항공사 및 철도 웹 사이트 / 앱

6.5.2. 인증 메커니즘

이러한 모든 시스템은 자체 인증 기법을 고안해 냈다. 대다수의 사용자는 Username + Password 시스템을 사용한다. 그들 중 일부는 일회성 (One Time Password) 인증을 기본 요소 또는 두 번째 요소로 가지고 있다. 이 외에도 PKI는 지난 10 년 동안 안전한 인증 격차를 충족시키는 데 중요한 역할을 담당해 왔다. 여러 은행 시스템에서 PKI는 기업 자금 이체에 대한 두 번째 요소 인증이다. e-Tenders와 같은 정부 플랫폼의 경우 PKI는 기본 인증 및 데이터 암호화에 중요한 역할을 한다. 최근 과거에 Aadhaar는 최신 시스템에서 쉽게 사용할 수 있는 (Open API) 인증 모델이 되었다.

6.5.3. 개발 동향

Aadhaar는 인도에서 가장 중요한 개발 중 하나이며, 시민들의 신원 파악에 정부의 강조가 계속되고 있다. 대부분의 Aadhaar 데이터에는 인증 된 인구 통계 정보 및 사진과 함께 등록 된 모바일 및 이메일 ID가 있다. 따라서 생체 인식 / OTP 기반 검증을 사용하여 온라인 인증 / KYC에 대해 인증 된 액세스를 제공하기 위해 채택되고 있다.
인도는 크고 정교한 국가 공개키 인프라 (PKI)로도 유명하다. 이것이 엄격하게 통제되는 반면, 국가 PKI 설정은 인도 정부가 규제하는 4개의 공인 인증기관과 3 개의 밀접한 그룹 인증 기관으로 구성 된다. 이 PKI의 인증서는 Adobe, Microsoft 및 PKI 기반 사용자 소프트웨어가 있는 다른 플랫폼에서 신뢰할 수 있다. 인도는 또한 PKI 사용자가 많다. 1,500 만 개 이상의 장기 디지털 서명이 여러 응용 프로그램에서 발행되어 사용되고 있다. 최근의 혁신으로 인해 전자 서명은 2,000 만 명의 사용자를 넘었으며 새로운 시스템이 정부가 규제하는 Open API로 쉽게 채택 할 수 있다. 최근의 물품 및 서비스 세금 (GST) 시스템은 약 1 천만 명의 사용자가 전자적으로 상호 작용하고 파일을 작성할 수 있도록 지원하는 PKI 사용자 중 가장 큰 시스템이다.

7. FIDO와 PKI 사례연구

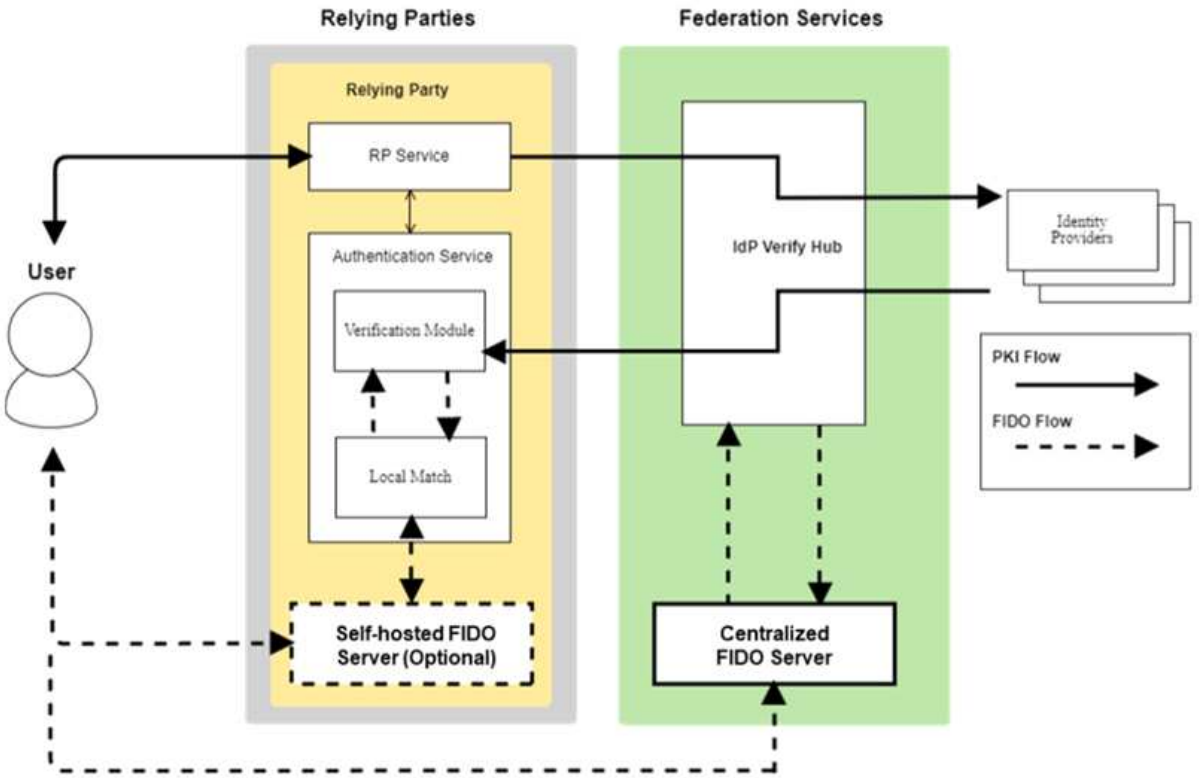
FIDO는 공개키 암호화를 기반으로 하는 표준 기반, 상호 운용 및 플러그 가능 인증을 위한 세계 최대의 에코 시스템이다. FIDO는 대부분의 모바일 장치 및 브라우저와 호환되므로 온라인 서비스의 보안을 향상시키는 동시에 기업 비용을 절감하는 데 적합하다. 전반적인 프로세스는 레거시 솔루션보다 간단하고 소비자에게 더 안전하다.
비록 FIDO와 PKI는 공개 키 암호화를 기반으로 하지만 각각은 다른 접근 방식을 취한다. FIDO는 사용자 인증이 필요한 다양한 수직 솔루션에 프로토콜을 적용한다. 이는 사용자의 개인 정보를 보호하는 데 초점을 맞추고 공개키 암호화 방법을 사용하여 사용자를 신뢰 당사자에게 인증한다. 자격 증명은 사용자 확인 (예 : 생체 인증 기반 또는 PIN 기반)으로 보호되며 일반적으로 기기 보안 요소에 안전하게 저장된다. 생체 인증은 암호화 계산을 수행하기 위한 개인키를 잠금 해제하기 위해, 로컬 인증을 수행하는 클라이언트 측에서만 필요하다. 사용자의 생체 인식 데이터는 장치를 떠나지 않으므로 인증하는 동안 필수 정보만 인증 서버 및 신뢰 당사자와 공유한다. 사용자, 키 쌍 및 신뢰 당사자는 FIDO가 신뢰 당사자 당 하나의 키 쌍을 사용하고 전역 상관 조정 사용을 피하는 것을 의미하는 튜플이다. FIDO 프로토콜의 설계 원칙은 여러 신뢰 당사자 간에 사용자의 동작을 추적 할 수는 없다.
수행되어야 할 신원 바인딩은 FIDO의 범위를 벗어나 요구 사항이나 규정에 따라 구현될 수 있다.

반면에 PKI 시스템은 인증 기관 (CA), 등록 기관 (RA) 및 검증 기관 (VA)과 같은 신뢰할 수 있는 제 3 자의 참여로 디지털서명법의 필요성을 해결한다. 또한 PKI에는 디지털 인증서를 해지하거나 공개 키 암호화를 관리 할 때뿐만 아니라 프로세스를 생성, 관리, 배포, 실행, 저장하는 일련의 정책과 절차가 포함되어 있다. 하나의 인증서가 여러 신뢰 당사자와 관련이 있으므로 인증서의 해지 및 유효성 검사가 필요하다. PKI의 목적은 전자 상거래, 인터넷 뱅킹, 전자 정부 등과 같은 다양한 네트워크 활동에 대한 정보의 안전한 전송을 하는 것입니다.

PKI 솔루션을 배포 할 때 복잡성과 실질적인 문제로 인해 신분 연합 서비스가 등장하고 이러한 신뢰 문제를 해결하는 것이 목표이다. 그러나 신분 연합은 신원 정보의 정의가 모든 당사자에게 명확하고 유사하게 이미 알려진 당사자들로 구성된 작은 트러스트 circle에서 보다 잘 작동한다. 예를 들어, 뱅킹에 대한 신분 연합 서비스는 사용자가 제공한 신원의 정보가 식별 목적을 위해 다른 은행에 쉽게 매핑 될 수 있기 때문에 사용자가 다른 은행에 자신을 식별하도록 허용한다.

PKI는 지정된 특성을 사용하여 세계적으로 인정 된 자격 증명을 만들려고 시도하지만 PKI를 신분 연합 서비스와 결합하는 것이 적합하다. 또한 PKI를 사용하는 트러스트 루트는 기존 트러스트 서클을 확대하고 약한 신뢰 관계를 강화하기 위해 신분 연합 서비스에 쉽게 통합 될 수 있다. 특정 사용자에 대한 세분화 된 프로필을 원하는 개인 신뢰 당사

자의 경우 FIDO는 PKI 에코 시스템으로 보완되어 신뢰 당사자간 강력하고 표준화 된 ID 바인딩이 존재할 수 있다. 우리는 아래에 식별 및 인증 흐름을 묘사했다.



(그림 7-1) 계정 Federation 흐름 (출처: APKIC)

RP 서비스에 접근하는 사용자는 자신의 PKI 자격 증명과 개인키 소유 증명을 RP 서비스에 먼저 제공해야 한다. 그러면 RP 서비스가 자격 증명을 IdP 검증 허브에 넘긴다. 자격 증명은 사용자가 보유한 PKI의 종류에 따라 통신, 은행 또는 정부 IdP와 같은 신원 제공 업체로 전달된다. FIDO 서버는 PKI 공급자가 중앙 집중 방식으로 배포하거나 신뢰 당사자가 자체 호스팅 할 수 있다. 이 두 배포 모델의 차이점은 비즈니스 요구 사항, 사용자 경험 및 규정 준수에 따라 달라진다.

사용자 편리를 향상시키길 원하는 RP 는 PKI 식별에 (자체 호스팅 FIDO 서버 사용)에 기반한 초기 신원 바인딩 단계 이후에 FIDO를 기본 인증 방법으로 선택할 수 있다. 이러한 방식으로 전반적인 PKI 인증 시간이 단축되고, 사용자가 자연스럽고 원활하게 스마트폰에서 인증을 수행 할 수 있다. 간단히 말해서 PKI는 사용자의 신뢰와 근본적인 기본 특성을 제공하지만 FIDO는 이러한 기반을 보완 할 수 있으며 표준 인증 보안 요구 사항 및 솔루션 인증 프로세스 적용으로 성능과 사용자 편리를 향상시킬 수 있다.
FIDO와 PKI는 모두 동일한 공개 암호화를 기반으로 하므로 FIDO와 개인정보 보호 원칙을 위반하지 않는 PKI 시스템간 공통 암호화 구성 요소를 공유 할 수 있으며 키 크기, 암호 알고리즘, 키 생성 절차, 키 보호등을 포함한 암호화 키의 보안 요구 사항을 충족한다.

7.1 한국 KISA의 K-FIDO(FIDO+NPKI 인증)

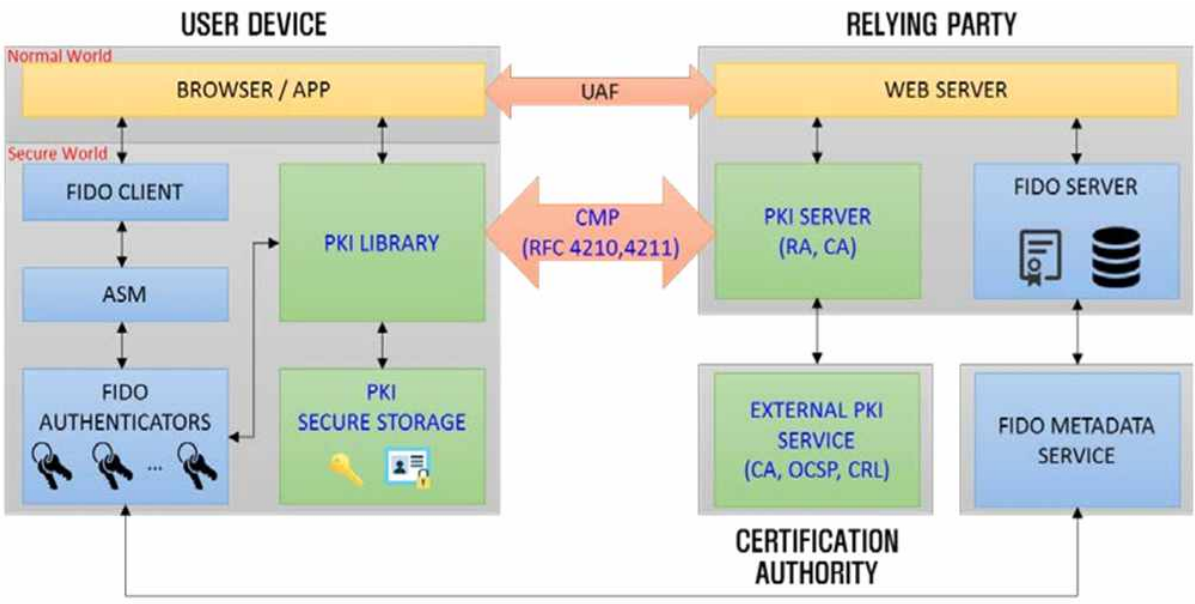
온라인 생활의 중요성이 커짐에 따라 식별 (주민등록증) 및 서명 (인장, 사인 등)의 역할을 하는 온라인 수단을 제공해야한다.

<표 7-1> 국내 온/오프라인 인증관련 기술

	온라인	오프라인
관련 법률 증거	디지털 전자서명 행위	주민등록 관련 법령
	Identification + 전자서명	주민 등록증 + Seal(Autograph)

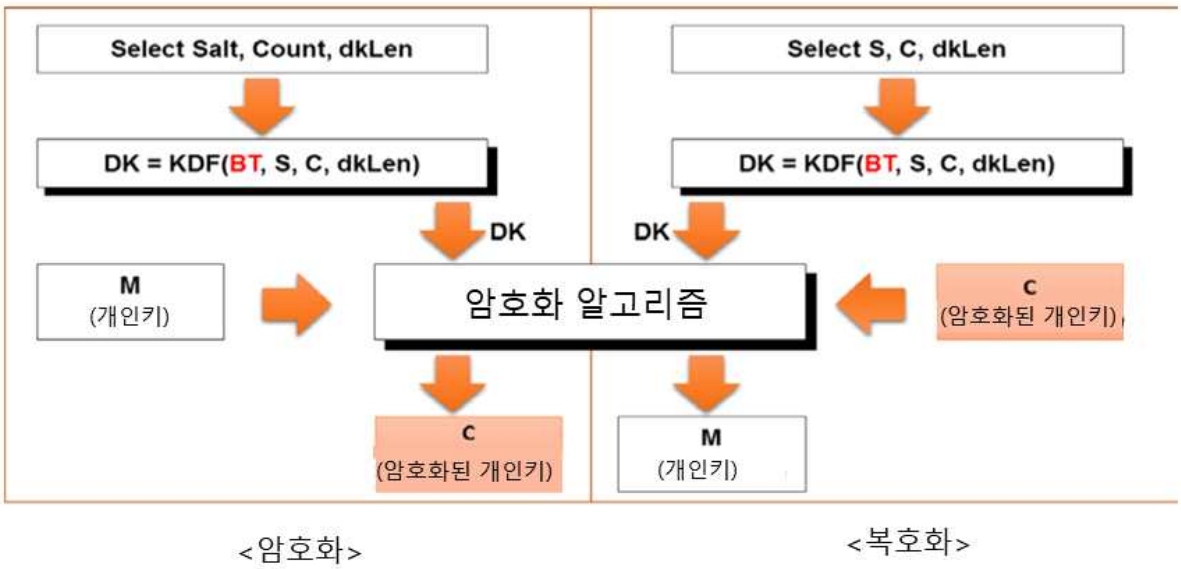
공인 인증서는 신원을 확인하고 전자 문서의 변조를 방지하고 온라인 거래의 진위 여부를 확인하는 보안 수단으로 사용된다.
최근 ICT 환경이 유선에서 모바일 장치로 변경됨에 따라 편리하고 안전하며 사용하기 쉬운 공인 인증서의 수단을 제공해야한다는 요구가 커지고 있습니다.

K-FIDO 기술은 사용자가 암호 및 ActiveX 설치를 입력하지 않고 등록 된 생체 인식 데이터를 사용하여 인증서를 사용할 수 있게 한다. FIDO 표준의 변경을 최소화하기 위해 FIDO와 FIDO UAF 프레임 워크에 인증서 링크 기술 프레임 워크가 추가되었다. 그래서 K-FIDO 기술은 과기정통부 인증서를 사용하는 응용 프로그램에 대해 필요한 경우 사용자 인증 및 디지털 서명을 위해 별도의 공개 키 쌍을 사용한다. K-FIDO 기술은 FIDO 구조 또는 UAF 프로토콜을 변경하지 않고 확장 메시지를 사용하여 인증서와 연결된다.



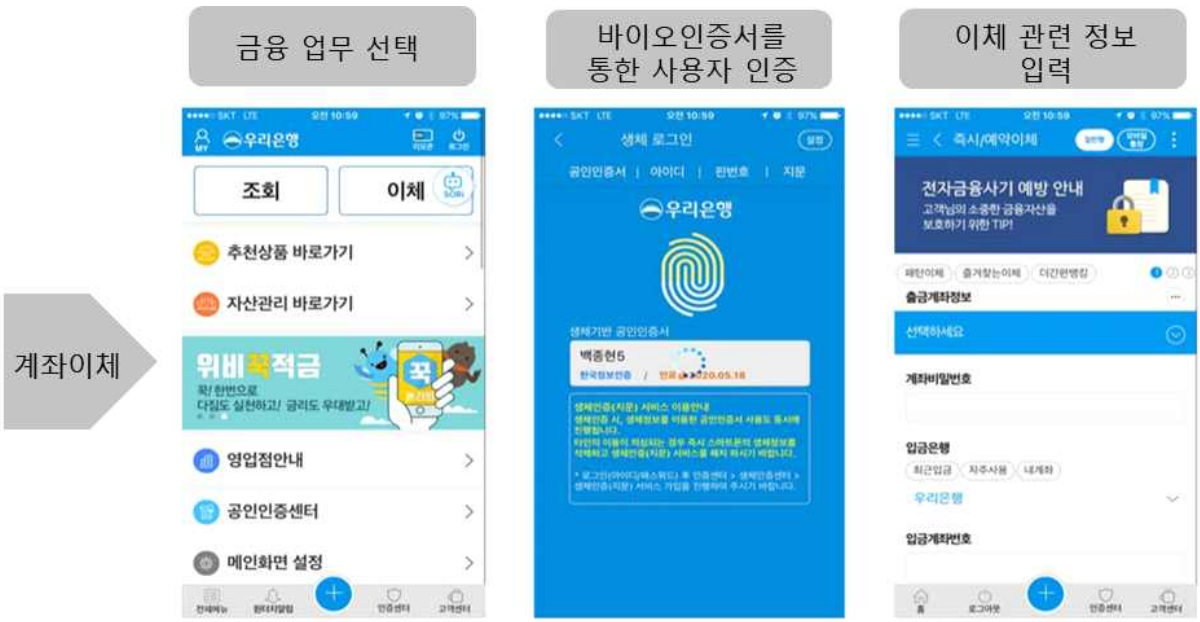
(그림 7-2) K-FIDO 개요 (출처: APKIC)

FIDO 인증 기술을 통해 사용자는 암호를 입력하지 않고 등록 된 생체 인식 데이터를 사용하여 인증서를 사용할 수 있다 (PKCS # 5 및 # 8 사양 사용).



(그림 7-3) 생체기술의 결합을 통한 PKI 키 쌍의 보호 기법

현재 K-FIDO 기술은 지문 및 홍채와 같은 등록 된 생체 인식 데이터를 사용하여 일부 모바일 뱅킹 서비스에 적용되었습니다.



(그림 7-4) K-FIDO 실 사례 (출처: APKIC)

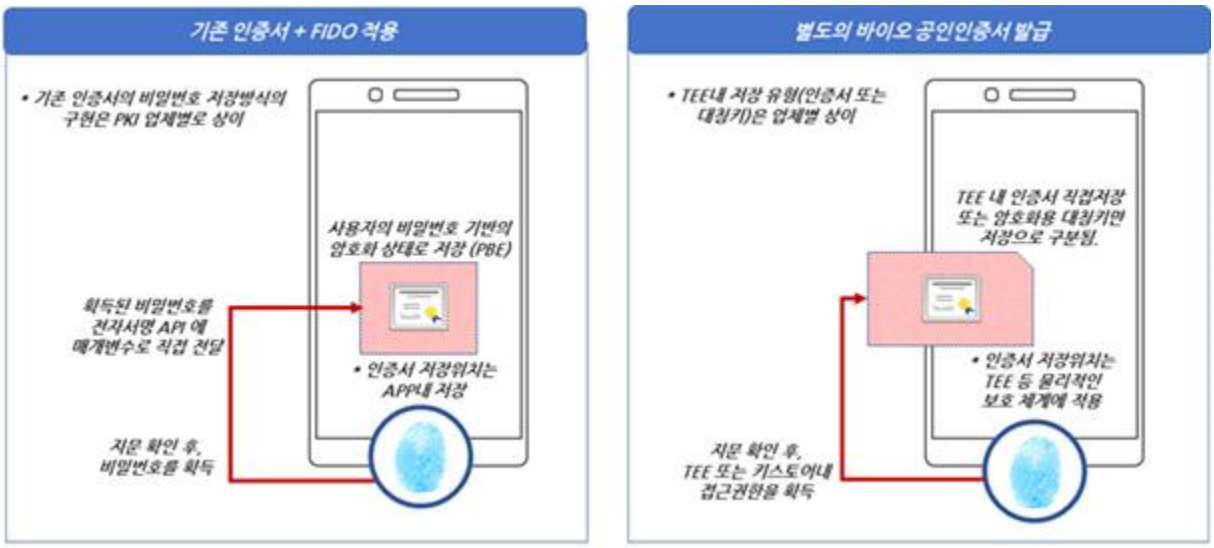
7.1.1 공인인증서와 FIDO 기술의 결합

기존 공인인증서의 체계는 안전한 사용 환경을 확보하고자, 공인인증서의 소유주 확인을 위해 비밀번호와 같은 지식기반의 검증 절차를 수행하고 있다. 이는 PBE(Password

Based Encryption) 방식의 보호 체계로써, 결국 사용자가 기억 및 입력을 해야 하는 불편함에 기반한다.

핀테크를 통한 사용자 위주의 서비스 컨텐츠 및 사용자 주도형 서비스의 확산으로 모든 서비스에서는 사용자의 편의성을 가장 최우선적으로 고려하고 있다. 이러한 흐름에 비추어 기존의 공인인증서 체계도 결국은 지식기반 및 입력에 기반하는 흐름을 생체기반으로 전환하여, 사용자의 편의성은 향상시키되 기존의 보안성은 그대로 유지하는 방향으로 전환이 되고 있습니다.

공인인증서의 비밀번호 체계를 FIDO 기반으로 대체하는 부분은 크게 두가지 형태로 구분이 된다.
첫 번째는 기존 공인인증서 그 자체를 사용하되, 비밀번호 영역의 보호 및 사용 체계만을 FIDO 기반으로 전환하는 것이고, 두 번째는 기 사용 공인인증서가 아닌 별도의 공인인증서를 새로이 발급받아 사용하되, 인증서의 저장 위치 자체를 물리적으로 안전한 영역 (예: Secure Element, USIM 등) 에 저장하는 방안으로 구분할 수 있다.

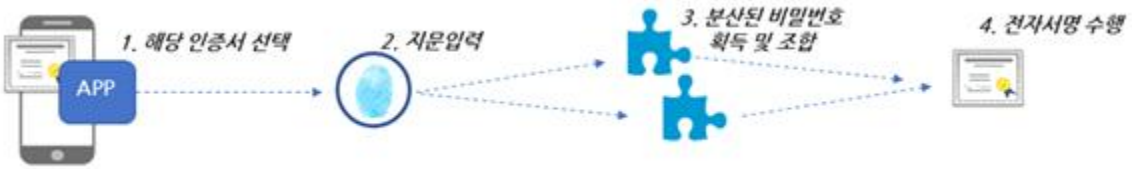


(그림 7-5) Biometrics를 결합한 공인인증서 적용 유형

7.1.1.1 공인인증서 비밀번호 대체로써의 FIDO 기술 결합

기존 공인인증서를 활용하여, 비밀번호만을 FIDO 기반으로 전환하는 방식이며, 이를 통해 사용자는 별도의 추가 발급없이 기존 인증서의 비밀번호만을 지문으로 대체할 수 있는 편의성을 확보한다.
단, 기존 1년 유효기간의 인증서를 그대로 사용한다는 부분과 해당 앱 외에도 다른 앱 또는 다른 디바이스 등에도 해당 인증서가 기존방식으로 저장 되어 있기 때문에, 최상위 보안 등급으로는 인정을 받지 못하고 1년 유효기간으로 유지가 된다.

(그림 7-6) 비밀번호의 지문 전환 등록 과정

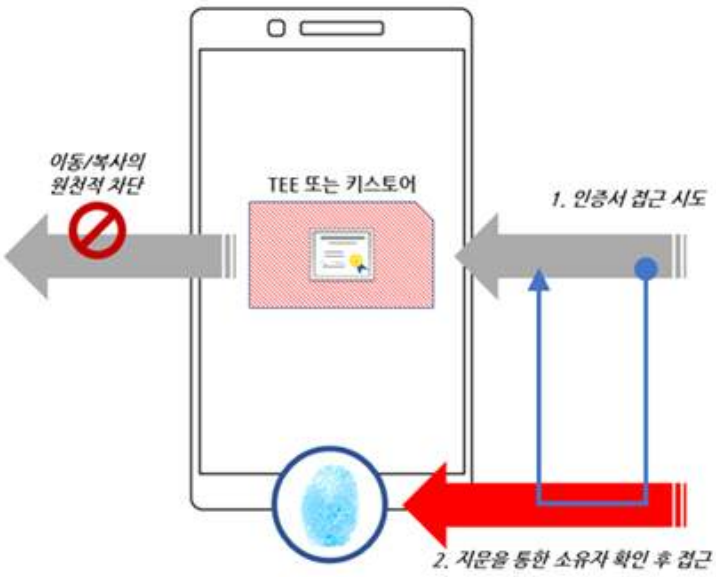


(그림 7-7) 지문을 통한 공인인증서의 전자서명 수행

7.1.1.2 공인인증서(발급, 보관, 사용) 전체적인 체계 내 FIDO 기술 결합

기존 인증서 체계가 아닌, 발급부터 보관, 사용까지의 전체적인 프로세스에 대해 안전한 영역을 최대한 활용하여 공인인증서의 안전한 사용환경을 마련한다.
이를 위해, 기존 인증서와는 별개의 인증서를 발급 받아야 하며, 이는 소유자의 확인을 생체기반으로 하여 높은 수준의 보안성을 확보하는 부분이 필요하다.

해당 인증서 자체가 유일성의 보장 (이동 및 복사의 금지) 및 생체기반의 결합이라는 보안성을 갖게 됨으로 기존 공인인증서 대비 높은 수준(유효기간 3년)을 확보 하게 된다.



(그림 7-8) PKI와 FIDO 결합의 기본 사상

7.1.2 바이오 공인인증서

7.1.2.1 K-FIDO 특징

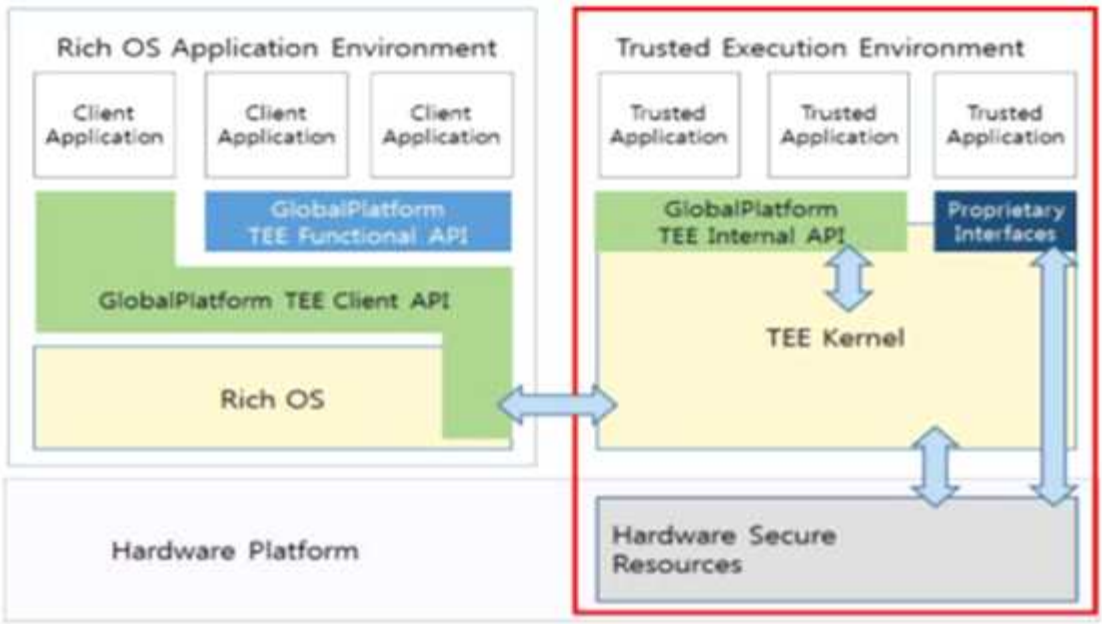
K-FIDO는 안전한 공인인증서 사용을 위해 KISA에서 제시한 “바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인”을 준수하는 공인인증서 체계 모델이다. 해당 모델에서는 사용자가 전자서명생성을 위해 비밀번호의 입력 대신 다양한 인증수단을 사용하는 방식을 표현한다.

7.1.2.2 안드로이드 운영 체제에서의 K-FIDO 적용

안드로이드 운영체제에서는 TEE 또는 키스토어를 활용하는 것을 권고한다. 공인인증서의 키쌍에 대해 TEE(또는 키스토어)내 직접 저장을 하거나, 해당 키쌍을 TEE(또는 키스토어)내 저장된 비밀키로 암호화 후, 암호화된 키쌍을 앱내 저장하는 형태로 구현 할 수 있다.

키스토어의 경우, 안전한 TEE영역내 구현되어 아래와 같이 물리적인 안정성을 보장받는다.

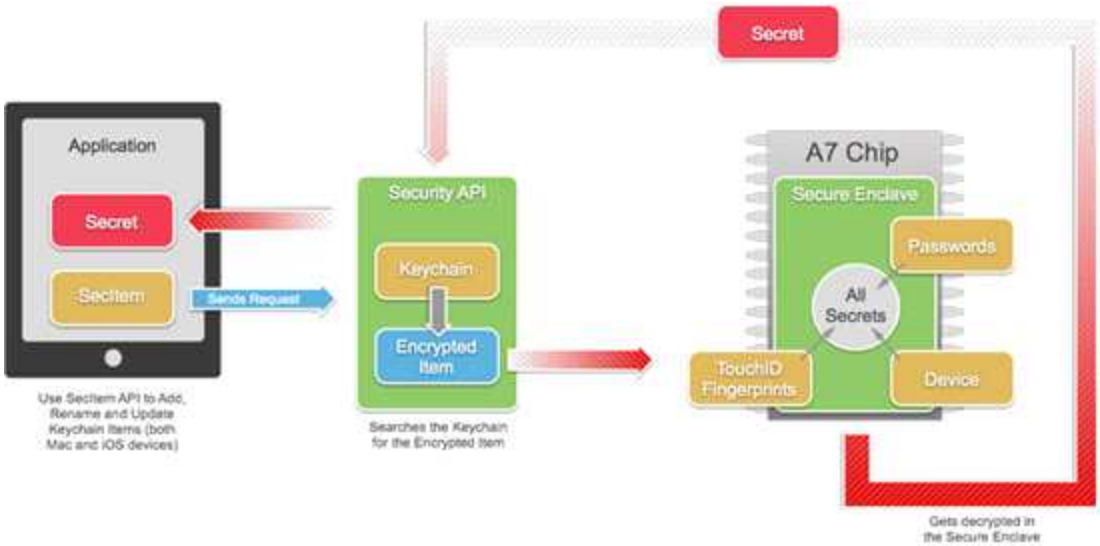
그러나, 일부 구 버전의 경우에는 TEE영역의 미사용 단말도 존재함으로 상기 방식의 적용을 위해서는 지원 대상의 범위를 정의하여야 한다.



(그림 7-9) 안드로이드 운영 체제내 TEE 기술

7.1.2.3 iOS 운영 체제에서의 K-FIDO 적용

iOS 운영체제에는 안드로이드 운영 체제와 유사한 키체인 영역을 통해, 키쌍을 보호하며, 해당 키쌍의 접근 제어를 위해 지문 또는 FaceID와 같은 안면 인증 기술을 활용한다.



(그림 7-10) iOS 운영 체제내 TEE 보호 기술

7.1.2.4 바이오 공인인증서 기술 분석

바이오 공인인증서는 현재 삼성Pass 방식과 국내 PKI 업체에 의해 구현된 두 가지 모델이 존재한다. 두가지 모델은 해당 키쌍의 저장 방식에 의해 약간의 차이가 있으며, 본 보고서에서는 PKI 업체에 의해 구현된 사례를 분석한다.

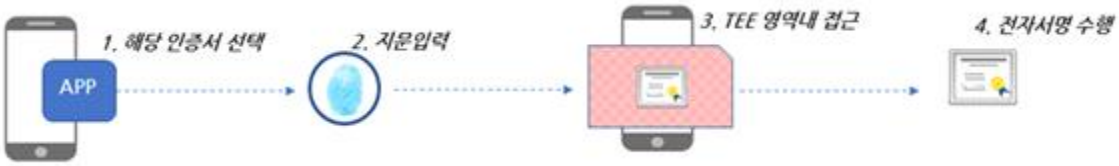
7.1.2.5 바이오 공인인증서 사례 분석

바이오 공인인증서 체계는 사용자에게 사용의 편의성 향상과 보안성을 모두 충족하는데 큰 의미를 부여하지만, 실질적인 서비스를 제공하는 금융권에서는 기존의 인프라 변경을 최소화하여 적용하는 것이 가장 큰 고민 사항이다. 이에 사용자와 관련된 클라이언트 영역 위주로 기술이 적용되고, 그 뒷단에서 수행되는 공인인증기관(CA)를 연계한 인증서 발급, 전자서명문 검증 및 유효성 검증 체계는 기존의 표준 체계를 수용하여 구현이 되어 있다.

현재 바이오 공인인증서의 적용 사례는 삼성Pass 형태와 PKI 업체에 의해 구현된 방식으로 구별해 볼 수 있다. 삼성Pass의 경우, 우리은행에 적용된 사례가 대표적이며 공인인증기관(CA)은 한국 정보인증을 연동한다. PKI 업체에 의해 구현된 경우, 부산은행(금결원 연동), 신한은행(증권전산 연동)에서 적용한 사례가 있다
해당 구현사례는 KISA의 실질심사를 모두 완료한 방식으로써, 상세 흐름은 아래와 같이

표현한다.

(그림 7-11) 바이오 공인인증서 발급



(그림 7-12) 바이오 공인인증서를 사용한 전자서명 수행

바이오 공인인증서는 편의성, 보안성 향상과 더불어 기존 인증서 체계와의 호환성 확보를 위해, CMP발급, 전자서명, 서명문 검증에 대해 표준을 준수한다.

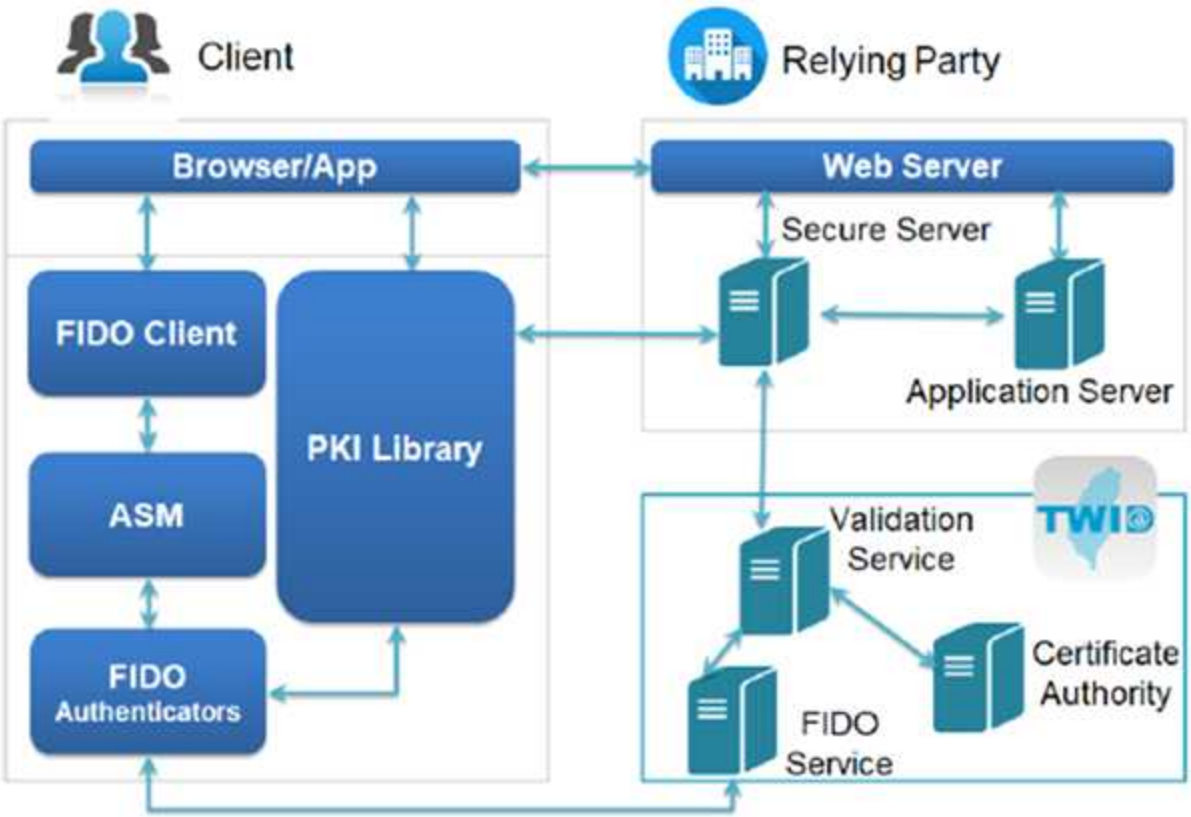
FIDO 표준 기술로는 국내 대다수 환경에서 사용하는 PKCS#7 기반의 전자서명을 충족하지 못하기 때문에, 이에 대한 해결을 위해 인증용 키(FIDO 키)와 별개의 거래용 키(공인인증서 키)를 분리하여 사용한다.

7.2 대만 TWCA의 PKI와 FIDO를 활용한 인증센터

7.2.1 TWCA

TWCA은 은행, 주식 보안 회사, 증권 투자 신탁 및 컨설팅 회사, 정부 기관 등 금융 산업에 PKI 기술을 적용한 보안 솔루션을 제공한다. 현재 사용자는 암호가 있는 인증서를 사용해야 한다. TWCA은 FIDO 솔루션으로 사용자 편의를 향상시키고 기대한다. TWCA은 인증기관 구성 요소와 FIDO UAF 구성요소를 통합하고, 이는 사용자가 FIDO UAF 로컬 인증 기능을 사용하도록 도와준다. FIDO의 로컬 인증 기능은 이미 여러 가지 생체 인식 기술을 채택 해 사용자가 지문, 홍채 또는 기타 생체 인식으로 인증서를 보다 쉽게 사용할 수 있도록 한다.

7.2.2 TWCA를 통한 FIDO 기술 분석



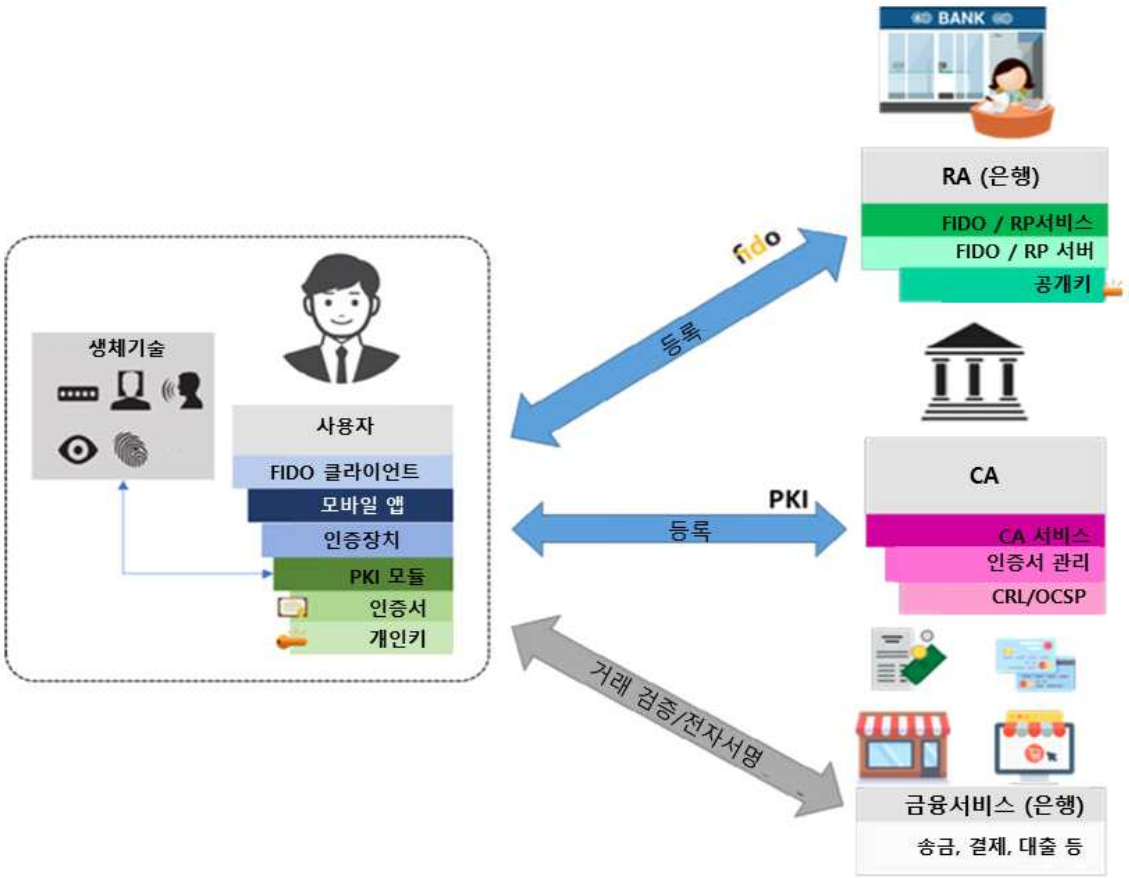
(그림 7-13) 대만에서의 FIDO와 PKI 연동 개요 (출처: APKIC)

TWCA은 또한 더 많은 온라인 인증 방법을 개발했다. 사용자는 e-ID, 은행 계좌 및 기타 도구를 사용하여 TWCA의 ID 서비스로 온라인 인증서를 적용 할 수 있다. TWCA은 여러 명의 ID 파트너와 연결하기 위해 기관 고객에게 단일 포털을 제공하고 최종 사용자는 TWCA의 서비스를 통해 ID 정보를 온라인으로 입력 할 수 있다.

TWCA은 파트너와 더 많은 응용 프로그램을 개발하는 TWID 플랫폼을 시작했으며 TWID 응용 프로그램을 사용하여 인증서를 여러 응용 프로그램에 적용 할 수 있다. 예를 들어 인증서를 전자 투표에 적용하고 TWSE (Taiwan Stock Exchange) 및 TFE (Taiwan Future Exchange)에서 개인 투자 기록을 조회 할 수 있다.

7.3 태국의 PKI와 FIDO를 활용한 금융서비스

아래 그림에서 은행 고객은 공개 키 시스템에 등록하고 지역 은행 지점에서 인증서를 취득하기 위해 휴대폰을 직접 등록해야 한다. 이후 고객은 휴대폰을 사용하여 은행 거래 및 문서 서명을 인증 할 수 있다.



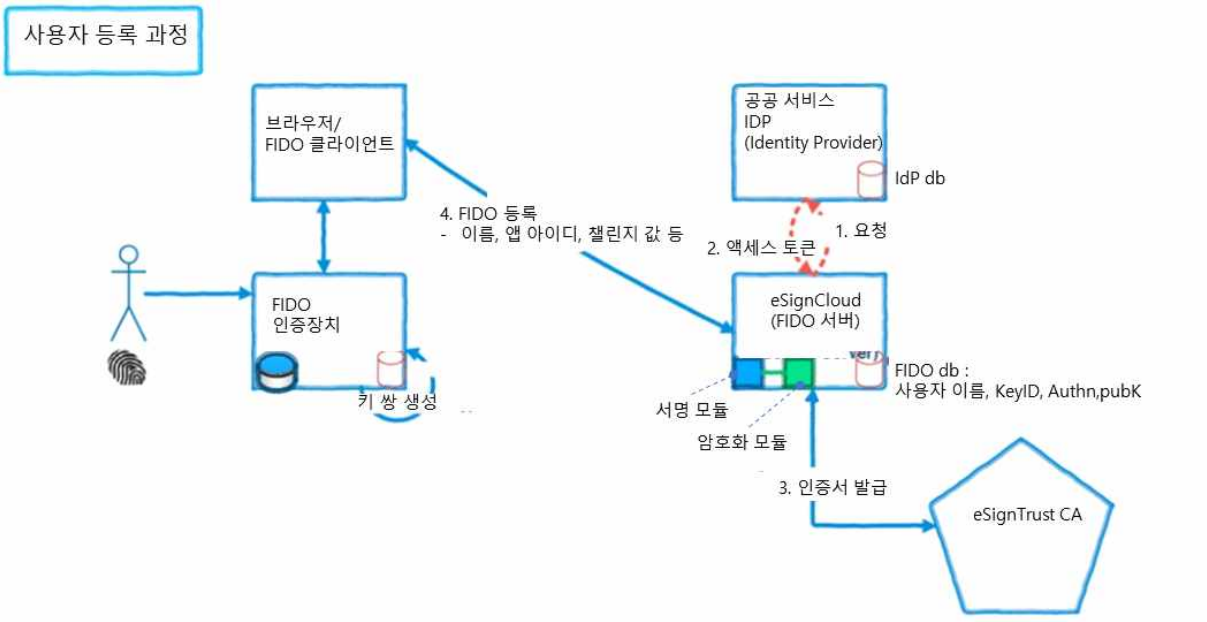
(그림 7-14) 태국에서의 FIDO와 PKI 연동 (출처: APKIC)

7.4 마카오의 FIDO를 활용한 eSignTrust eSignCloud

■ 사용자 등록 프로세스

1) eSignCloud가 Gov.IdP (인증 서버)를 통해 승인 요청한다.
2) eSignCloud가 Gov.IdP로부터 평가 토큰을 받고 액세스 토큰 정보를 사용하여 eSignCloud 계정을 생성한다.
3) eSignTrust RA가 eSignTrust 인증기관에서 eSignCloud 인증서를 등록한다.
4) 사용자가 eSignCloud에 로그인하여 FIDO 및 서명자의 서명 활성화 데이터 등록을 시작한다.

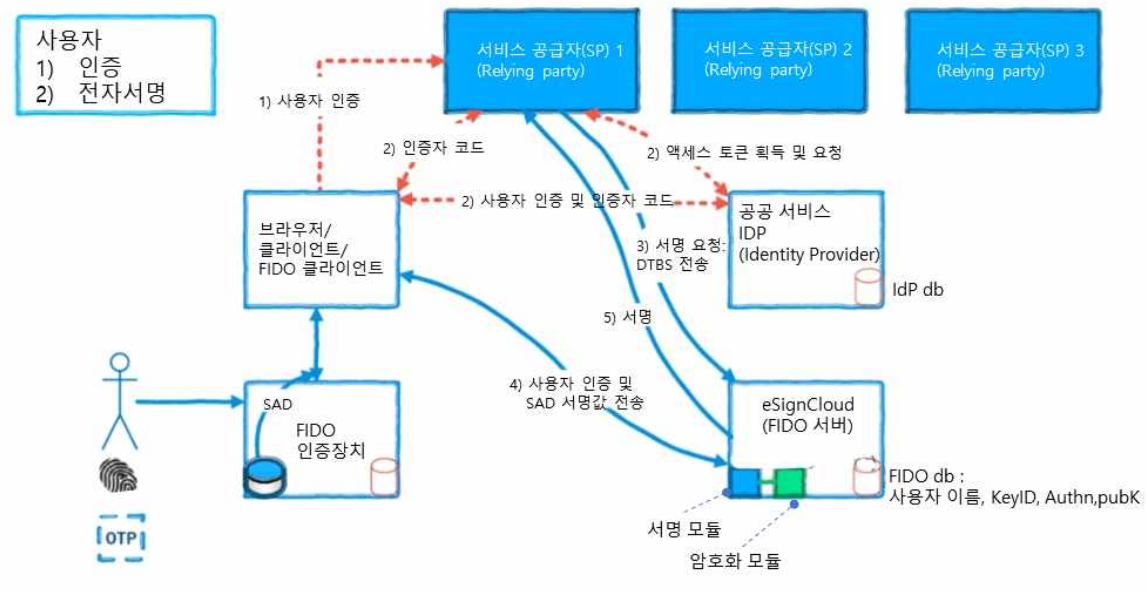
아래의 그림은 사용자 등록과 관련된 상세 프로세스를 보여준다.



(그림 7-15) eSignTrust eSignCloud Service를 연계한 FIDO 등록 과정 (출처: APKIC)

■ 사용자 인증 및 서명 프로세스

1) (선택 사항) 사용자가 SP 응용 프로그램에 로그인한다.
2) (선택 사항) SP 권한 부여 프로세스 :
   a. SP가 IdP (Gov.Services)에 인증 요청을 보낸다.
   b. SP는 사용자 에이전트를 IdP (Gov.Services)로 리디렉션하여 인증을 제공한다.
   c. 사용자 에이전트는 IdP (Gov.Services)로부터 인증 코드를 얻는다.
   d. 사용자 에이전트는 인증 코드를 SP로 보낸다. SP는 인증 코드로 액세스 토큰을 얻는다.
3) 사용자가 서비스에 서명을 요청하면 SP는 DTBS (Data To Be Signed)를 계산하여 eSignCloud로 보낸다.
4) eSignCloud FIDO Server는 FIDO 클라이언트에게 FIDO 인증 요청을 보낸다. FIDO 클라이언트는 FIDO 인증장치(Authenticator)를 통해 FIDO 클라이언트의 개인키 액세스 권한을 획득한다. 성공하면 FIDO 클라이언트는 FIDO 클라이언트의 개인키로 서명 활성화 데이터(SAD)에 서명하고 SAD를 포함한 인증 응답을 eSignCloud에 보낸다. 5) eSignCloud Signature Activation Module은 SAD를 확인하고 Crypto Module에 대한 서명을 활성화한다. eSignCloud가 서명 값을 SP로 보낸다.



(그림 7-16) 사용자 인증과 전자서명 과정 (출처: APKIC)

7.5 인도 Aadhaar, PKI와 FIDO

Aadhaar 및 기타 신원 플랫폼은 현재 여러 트랜잭션에 대해 ID 확인 기능을 지원한다. 은행이나 기업과 같은 조직에서는 자체 검증 된 사용자 기반을 가지고 있다. 따라서 질문 / 정보 검색을 통해 데이터베이스 내에서 간단한 ID 증명 시스템을 쉽게 노출 할 수 있다. 이들 모두는 FIDO가 초기 등록에 필요로 하는 필수 ID 확인 지원을 제공 할 수 있다.
PKI 시스템은 신원 확인 서명, 데이터 암호화, 법적 구속력, 부인 방지, 철회 및 시스템의 기타 요구 사항 및 법적 규정에 대한 자체 역할을 수행한다.

FIDO는 해당 시스템 내에서 사용자 인증의 필요성을 충족시키는 데 중요한 역할을 수행할 수 있다. 이러한 사용자 인증 / 유효성 검사는 반복되는 활동이며 현재 시스템 대부분 온라인 상태인 대체시스템에 의존합니다. 이것은 인구 통계 정보 또는 인증 매개 변수가 인터넷을 통해 반복적으로 이동해야하므로 의존성과 위험을 노출시킨다. FIDO는 사용자를 로컬에서 인증하고 이러한 시스템에서 요구하는 보안 요구 사항을 충족하는 주요 장점을 제공한다.

이 개념에 보충하면, FIDO Alliance는 FIDO 인도 워킹 그룹을 설립했으며 워킹 그룹과 일부 인도 인증 기관은 여러 은행 시스템 및 기타 인증 플랫폼에서 FIDO 가능성을 논의했다.
새로운 또는 기존 시스템이 FIDO 인증을 채택하려면 현재 방법론과 공존하는 것이 중요하다. 이 방법을 통해 각 방법의 장점을 다음과 같이 고려해야 한다.

■ 기존 시스템을 사용하여 ID를 증명
- 사용자는 조직의 기존 모델을 사용하여 시스템에 탑재되다.
- 이것은 일회성 등록 확인이다. 별도의 시스템이나 검증 메커니즘이 필요하지 않는다.
- National ID (Aadhaar)는 ID / 주소 정보와 함께 등록 할 때도 사용할 수 있다.
- 이것은 즉각적으로 인증을 만든다.

■ PKI (Public Key Infrastructure)
- 공인 PKI로 일회 인증을 통한 공개 키 암호화
- 정부의 검증된 인도 PKI 인증서 정책
- 각 '거래 확인'에 대한 법적 유효성. 법원에서 부인 방지 바인딩이 있는 경우 유효
- 만료, 중앙 집중식 해지 등의 이점이 있는 중앙 인증 플랫폼

■ FIDO
- 간단한 트랜잭션 확인
- 등록 및 인증 메커니즘을 위한 PKI + National ID와의 혼합
- 클라이언트와 서버 간의 강력한 인증 거래 중 외부 의존성 (본질적으로 반복적). 매번 National ID 인증 또는 전자 서명에 의존하지 않는다.
- 탁월한 사용자 편의

부 록 Ⅰ-1

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서(1)

- 해당 사항 없음

Ⅰ-1.2 지식재산권 확약서(2)

- 해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 기술보고서가 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

- 해당 사항 없음

Ⅰ-2.2 시험표준 제정 현황

- 해당 사항 없음

부 록 Ⅰ-3

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

본 기술보고서의 연계(family) 표준

- 해당 사항 없음

부 록 Ⅰ-4

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

참고 문헌

- 해당 사항 없음

부 록 Ⅰ-5

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

영문기술보고서 해설서

- 해당 사항 없음

부 록 Ⅰ-6

(본 부록은 기술보고서를 보충하기 위한 내용으로 기술보고서의 일부는 아님)

기술보고서의 이력

판수	채택일	기술보고서번호	내용	담당 위원회
제1판	2018.0X.0X	제정 TTAx.xx-xx.xxxx	-	개인정보보호/ID 관리 및 블록체인 보안(PG502)