JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 21, No. 7 : 1411~1419 Jul. 2017

PKI 인증과 FIDO 인증에 대한 비교 분석

박승철*

A Comparative Analysis of PKI Authentication and FIDO Authentication

Seungchul Park*

School of Computer Science and Engineering, Korea University of Technology and Education, Chungnam 31253, Korea

요 약

PKI(Public Key Infrastructure) 인증은 개인키 소지(possession)와 개인키 보호 패스워드 지식(knowledge)이라는 2 요소 인증(2 factor authentication) 능력과 안전한 공개키 암호 프로토콜을 통해 인터넷 거래의 신뢰 인프라 구축에 많은 기여를 해왔다. 하나의 인증서로 모든 PKI 사이트를 접근할 수 있는 점도 PKI 인증의 활성화에 기여하였다. 그럼에도 불구하고 인증서 인프라 구축 비용, 인증서 관리에 따른 사용자 불편함, 그리고 개인키 보호 패스워드 관리의 어려움 등에 따른 여러 가지 문제점들이 노출되어 왔다. 최근에 주목받고 있는 FIDO(Fast IDentity Online) 인증은 PKI 인증과 같이 공개키 암호 프로토콜에 기초한 강력한 인증 서비스를 제공하면서도 사용자별 인증서 발급이 불필요하고, 생체 인증 등과 결합하여 안전하고 편리한 인증 서비스 제공을 추구하고 있다. 본 논문은 PKI 인증과 FIDO 인증의 동작 방식을 구체적으로 비교하여 각각의 장단점을 분석하고, 그에 따른 각각의 응용 분야를 제시하는 데 목적이 있다.

ABSTRACT

The two factor authentication capability, private key possession and key protection password knowledge, and the strong public key cryptography protocol of PKI authentication have largely contributed to the rapid construction of Internet transaction trusted infrastructure. The reusability of a certificate-based identity for every PKI site was another contribution factor of the spread of PKI authentication. Nevertheless, the PKI authentication has been criticised mainly for the cost of PKI construction, inconvenience of individual certificate management, and difficulties of password management. Recently FIDO authentication has received high attention as an alternative of the PKI authentication. The FIDO authentication is also based on the public key cryptography which provides strong authentication services, but it does not require individual certificate issuance and provides user-friendly and secure authentication services by integrating biometric technologies. The purpose of this paper is to concretely compare the PKI-authentication and FIDO-authentication and, based on the analysis result, to propose their corresponding applications.

키워드 : 중요 PKI, FIDO, 인증, 인증서

Key word : PKI, FIDO, authentication, certificate

Received 08 March 2017, **Revised** 08 March 2017, **Accepted** 17 May 2017

* **Corresponding Author** Seungchul Park(E-mail:scpark@koreatech.ac.kr, Tel:+82-41-560-1492)
School of Computer Science and Engineering, Korea University of Technology and Education, Chungnam 31253, Korea

Open Access https://doi.org/10.6109/jkiice.2017.21.7.1411 print ISSN: 2234-4772 online ISSN: 2288-4165

ⓒThis is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(http://creativecommons.org/li-censes/ by-nc/3.0/) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright Ⓒ The Korea Institute of Information and Communication Engineering.

Ⅰ. 서 론

2000년대에 들어오면서 공개키(public key)에 대한 인증서(certificate) 발급 및 관리 체계인 PKI(Public Key Infrastructure) 기반의 인증이 인터넷 뱅킹, 쇼핑몰 결제, 온라인 증권 거래, 공공 민원 서비스 등 많은 분야의 인터넷 서비스에 활발하게 사용되어 왔다. 특히 국가적인 PKI가 잘 구축된 우리나라에서는 2015년 말 기준으로 3,388만개의 인증서가 발급되어 광범위한 분야에서 사용되고 있다[1]. PKI는 높은 보안성이 증명된 공개키 암호(public key cryptography) 프로토콜에 바탕을 두고 있으며, 인터넷 사용 주체별 공개키를 신뢰할 수 있는 기관인 CA(Certification Authority)가 인증서 발급을 통해 보증하는 체계이다. 따라서 PKI 환경에서 특정 사용자의 인증서만 확인하면 해당 사용자의 공개키를 믿고 사용할 수 있으며, 인증서의 공개키에 대응되는 개인키(private key)로 작성된 서명 검증(signature validation)을 통해 인증서에 기술된 사용자임을 확인할 수 있다[2,3].

PKI 인증은 사용자가 인증서의 공개키에 대응되는 개인키를 소유(possession)하고 있음을 증명하고, 개인키가 해당 사용자만 알고 있는 패스워드 정보 등으로 안전하게 보호되고 있음을 보장하는, 2 요소 인증(2 factor authentication) 체계에 기초하고 있다. 보안성이 증명된 공개키 암호 체계와 결합된 PKI의 강력한 2 요소 인증 체계는, 기존의 패스워드 기반의 단일 요소 인증 체계를 대체하며 안전한 인터넷 거래를 위한 신뢰 인프라 구축에 많은 기여를 해왔다. 사용자가 하나의 인증서로 별도의 등록 절차 없이 모든 PKI 사이트에서 인증 받을 수 있는 점과, 공개된 인증서를 통한 서명 검증에 기초한 부인방지(non-repudiation) 서비스도 PKI 인증의 활성화에 기여하였다[4,5].

그럼에도 불구하고 PKI 인증은 PKI 인프라 구축을 위한 정책적 어려움과 높은 비용 부담, 개인별 인증서 발급과 유지 관리에 따른 불편함, 그리고 특히 개인키를 안전하게 보호하기 위해 개인이 별도로 관리해야 하는 패스워드에 대한 관리 어려움 등의 문제점들도 함께 노출해 왔다. PC의 파일 시스템과 같은 안전하지 않은 저장소에 개인키를 저장하고 패스워드로 보호하는 기존의 일반적인 개인키 보관 메카니즘은, 공격자가 비교적 쉽게 개인키를 복제할 수 있게 허용하고, 따라서 패스워드가 노출되면 개인키도 함께 노출되어 PKI의 2 요소 인증의 의미가 퇴색되게 한다. 이를 극복하기 위해 OTP(One Time Password) 시스템과 같은 추가적인 인증 도구의 도입을 필요로 하고, 이는 PKI 인증에서 사용자 불편을 가중시키는 또 다른 요인이 되고 있다[6,7].

최근에 FIDO(Fast IDentity Online) Alliance를 통해 표준화되고 보급되고 있는 FIDO 인증은, PKI 인증과 같이 공개키 암호 프로토콜에 기초한 강력한 인증 서비스를 제공하면서도 사용자별 인증서 발급이 불필요하고, 생체 인증(biometrics authentication) 등과 결합하여 안전하고 편리한 인증 서비스 제공을 추구하고 있다. FIDO 인증은 기본적으로 공개키와 개인키를 생성하고 개인키를 안전하게 보관하는 인증 장치(authenticator device)를 사용자가 소유하고, 지문 또는 홍채와 같은 생체 정보를 인증 장치에 입력함으로써 PKI와 같은 2 요소의 강력한 인증 서비스를 제공한다[8].

본 연구는 PKI 인증과 FIDO 인증의 동작 방식을 구체적으로 비교하여 각각의 특징을 분석하고, 분석 결과를 바탕으로 PKI 인증과 FIDO 인증에 적합한 응용 분야를 제시하고자 한다. 본 연구 결과를 통해 PKI 인증과 FIDO 인증이 적절하게 적용됨으로써, 인터넷 거래 인프라가 보다 안전하고 편리하게 개선될 수 있기를 기대한다.

Ⅱ. 관련 연구

PKI 기반의 사용자 인증은 [2]와 같이 표준 프로토콜인 SSL/TLS[9]의 클라이언트 인증(client authentication)을 활용할 수도 있고, 우리나라의 경우와 같이 공개키 암호 기반의 자체적인 인증 프로토콜(proprietary authentication protocol)을 사용할 수도 있다[3]. [10]은 SSL/TLS 기반의 PKI 인증과 우리나라 NPKI 기반의 인증을 비교분석하고 있다. PKI 인증을 위한 인증서와 개인키는 다양한 매체에 저장될 수 있지만, 2015년 12월 현재 우리나라에서는 3천8백만개의 이상의 인증서 중에 6.2%만이 HSM(Hardware Security Module)과 같은 안전한 하드 토큰(hard token)에 저장되고, 편의성 등의 이유로 대부분의 사용자는 HDD와 UDB 메모리와 같은 소프트 토큰(soft token)에 인증서와 개인키를 보관하고 패스워드로 보호하고 있음을 알 수 있다[11]. 소프

트 토큰과 하드 토큰 PKI 인증의 강도에 대해서는 [12]를 참고하기 바란다. 2012년에 결성된 FIDO Alliance는 2014년 U2F(Universal 2nd Factor)와 UAF(Universal Authentication factor) 등 2개의 표준을 발표하였다[13,14]. 본 논문은 패스워드 사용 없이 다중 요소(multi-factor) 보안 서비스 제공을 위해 제안된 UAF 표준을 중심으로 분석한다. FIDO 표준은 PayPal과 Alipay와 같은 대형 결제 대행 업체(PG-Payment Gateway)에 의해 채택되어 사용되고 있으며, 2015년 9월에는 BOA(Bank Of America)가 모바일 뱅킹에 FIDO 인증 적용을 발표하였다[15]. 우리나라의 경우에도 하나은행이 2015년 10월 FIDO 기반의 모바일 뱅킹 서비스 제공을 선언한 이후[16], 은행과 결제 대행사를 중심으로 FIDO 인증을 도입하였거나 도입을 서두르고 있다.

이와 같이 FIDO 인증이 기존의 PKI 인증의 대안으로써 결제 서비스뿐만 아니라 인터넷 뱅킹 서비스까지 부분적으로 적용되고 있지만, PKI 인증과 FIDO 인증에 대한 비교 연구는 거의 이루어지고 있지 않다. FIDO 인증은 공캐키 암호 프로토콜에 기초하고 있다는 점에서는 PKI 인증과 유사하나, 개인별 인증서에 기초하지 않는다는 점에서 PKI 인증과 확실한 차이를 가진다. 따라서 PKI 인증과 FIDO 인증이 적합한 응용 분야도 다를 수밖에 없다. 본 연구는 PKI 인증과 FIDO 인증의 차이를 구체적으로 분석하고, 각각에 적절한 응용을 제시하는 데에 초점을 맞추고 있다.

Ⅲ. PKI 인증

3.1. 인증서 발급 절차

PKI 인증은 공개키 암호 프로토콜을 사용하여 인증 대상 사용자의 개인키로 작성된 전자 서명(digital signature)을, 해당 사용자의 공개키를 사용하여 확인하는 작업이다. 따라서 PKI 인증의 핵심 문제는 사용자별 공개키가 해당 사용자의 공개키가 맞음을 증명하는 작업이고, PKI는 사용자별 공개키 인증서(public key certificate)를 신뢰할 수 있는 기관(CA-Certification Authority)을 통해 발급함으로써 이 문제를 해결한다. 우리나라의 대표적 CA는 금융결제원이다. 공개키 인증서 표준은 X.509[17]를 사용하고 있으며, 인증서 발급 절차는 그림 1과 같이 요약될 수 있다.

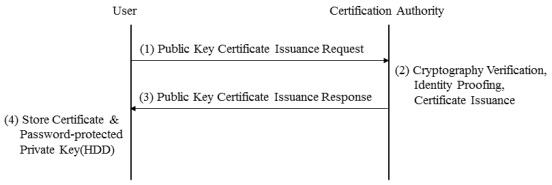

Fig. 1 PKI Certificate Issuance Procedure

사용자로부터 또는 등록대행 기관(예, 은행)을 통해 인증서 발급을 요청받은 CA는 요청된 공개키가 적절한 암호 프로토콜을 통해 생성된 키인지 검증하고, 인증서 발급을 요청한 소유자의 신원 정보의 진위를 확인한다(identity proofing). 신원 확인 방법과 절차는 인증서의 용도에 따라 달라질 수 있다. 예를 들어, 인터넷 뱅킹 용도로 사용될 인증서의 경우, 등록 대행 기관인 은행이 신원 확인 과정에서 신분증과 전화번호 등을 대면 과정으로 확인하고, 소유자의 은행 계좌 정보를 추가로 확인하여 공인인증서와 연결시킬 수 있다. 신원확인이 완료되면 CA는 공개키와 신원 정보(이름, 일련번호 등)가 기록된 인증서를 자신의 개인키로 서명함으로써 인증서를 발급한다. 인증서는 1년 정도의 유효기간을 가진다. 인증서를 발급받은 사용자는 보안 채널을 통해 인증서와 개인키를 특정 저장소(HDD/USB 메모리, 웹 저장소, HSM)에 저장하고, 패스워드 등을 통해 생성되는 암호키를 사용하여 개인키를 암호화한다.

3.2. 인증 절차

PKI 기반의 사용자 인증 절차는 적용되는 인증 프로토콜에 따라 다소 차이가 있으나, 일반적인 인증 절차는 그림 2와 같다. 서버는 먼저 클라이언트에게 사용자의 인증서를 요청하여 제공받는다. 인증서는 공개된 문서이므로 이 과정은 기밀로 수행될 필요가 없다. 인증서가 사전에 사용자 ID와 연계되어 서버에 등록되어 있는 경우 이 과정은 생략될 수 있다.

클라이언트로부터 인증서를 수신한 서버는 인증서를 발급한 CA의 공개키를 사용하여 사용자 인증서를 검증하고, 사용할 사용자 신원 정보를 추출한다. 인증서의 신원 정보가 서버의 서비스 제공에 충분하지 않을 경우 CA로부터 해당 사용자의 추가적인 신원 정보를 제공받을 수도 있고, 별도의 채널(온라인 또는 오프라인)을 통해 미리 수집한 후 인증서와 연결시킬 수도 있다. 서버의 추가적인 신원 정보 수집은 PKI 인증과는 별

개의 문제이다.

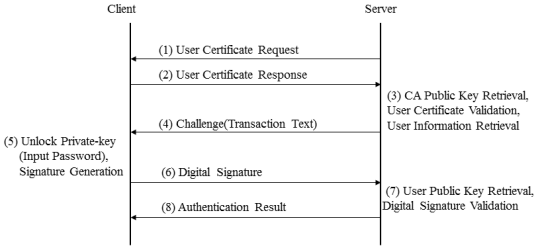

Fig. 2 PKI Authentication Procedure

인증서 검증과 필요한 사용자 정보 추출을 완료한 서버는 서명에 사용될 챌린지(challenge) 정보를 클라이언트에게 제공한다. 인터넷 뱅킹에서와 같이 거래 과정에서 거래 정보에 대한 인증(transaction authentication)이 필요한 경우, 거래 정보(transaction text)를 챌린지로 제공할 수 있다. 챌린지를 수신한 클라이언트는 사용자로 하여금 패스워드 입력 등으로 개인키를 해제하여, 챌린지에 대한 해시값(hash value)을 공개키 암호 프로토콜로 암호화함으로써 전자 서명을 생성하게 하고, 전자 서명을 서버에게 전송한다. 서버는 해당 사용자의 인증서로부터 공개키를 추출하여 수신한 전자 서명을 검증하고, 검증 결과에 따라 인증 결과를 클라이언트에게 전송한다.

Ⅳ. FIDO 인증

4.1. 인증서 발급 절차

PKI 인증과 같이 공개키 암호 프로토콜을 사용하는 FIDO 인증의 가장 큰 특징은, 사용자별 인증서를 발급하는 대신 사용자가 인증 시에 사용하는 인증 장치(authenticator device)의 생산자별로 인증서를 발급하는 것이다. 그림 3은 FIDO 인증서 발급 과정을 요약하고 있다. 인증 장치 생산자는 장치와 사양을 제공함으로써 FIDO 인증기관에 생산자 증명 인증서(attestation certificate) 발급을 요청한다. FIDO 인증기관은 인증 장치의 공개키 암호 프로토콜, 개인키 보호 메카니즘 등을 검증하고, 안전성, 호환성, 편의성 등의 측면에서 기준에 부합하면 생산자 증명용 공개키/개인키 쌍을 생성한 다음 증명 인증서를 발급한다.

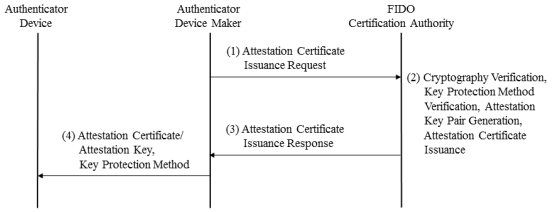

Fig. 3 FIDO Certificate Issuance Procedure

증명 인증서를 발급받은 생산자는 자신이 생산하는 인증 장치에 증명 인증서와 개인키를 안전하게 저장하고, 인증서 발급 과정에서 증명된 개인키 보호 메카니즘을 설정한다. FIDO 인증은 PKI 인증과 달리 보안성과 편의성이 높은 생체 인증(biometrics authentication)을 개인키 보호를 위한 기본 메카니즘으로 채택하고 있다.

4.2. 공개키 등록 절차

PKI 인증에서 사용자의 공개키는 인증서 발급과정에서 생성되어 CA에 한번 등록되는 데 비해, FIDO 인증에서 사용자의 공개키는 인증 장치에서 생성되어 서버별로 다르게 등록된다. FIDO 인증을 위한 공개키 등록 절차는 그림 4와 같다.

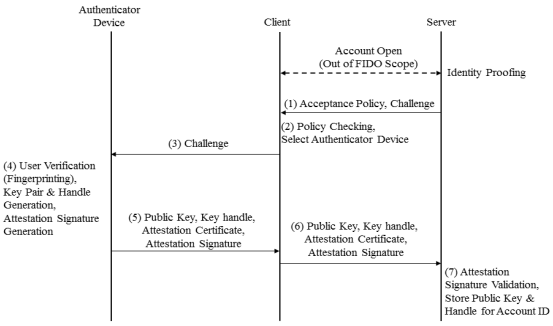

Fig. 4 FIDO Public Key Registration Procedure

FIDO UAF 표준에서는 서비스 제공자에 해당하는 엔티티를 RP(Relying Party)로 표현하고 있으나, 본 논문에서는 RP의 웹 서버 부분 등 FIDO 인증 동작과 관련이 적은 부분은 제외하고 FIDO 서버 부분만 표현하였다. 사용자 단에서도 FIDO 인증과 관계가 깊은 클라이언트와 인증 장치(authenticator) 부분만 표시하고, 웹 브라우저, 인증 장치와 클라이언트간의 인터페이스

인 ASM(Authenticator-Specific Module) 부분 등은 제외하였다. FIDO 인증에서 인증 대상 사용자의 계정 개설(account open) 작업은 사전에 완료되는 것으로 가정하고, 계정 개설 과정에서 이루어지는 사용자에 대한 신원 확인 방법과 절차는 서버에 따라 결정될 뿐, FIDO 인증과는 무관하다. 계정 개설을 완료한 서버는 서비스 수준에 맞는 인증 장치 수용 정책(acceptance policy)과 서명용 챌린지를 클라이언트에 전송함으로써 계정 인증에 사용될 공개키 등록을 요청한다. 등록 요청을 받은 클라이언트는 서버의 수용 정책에 맞는 인증 장치를 선별하여 사용자가 선택하게 하고, 챌린지를 선택된 인증 장치에게 전송한다.

인증 장치는 미리 설정된 사용자 확인 방법(예, 지문 또는 홍채 인식)으로 사용자를 인증(user authentication)하고, 인증이 성공하면 사용자 공개키와 개인키 쌍을 생성하고 서버 도메인에서 키를 유일하게 구분할 수 있는 키 핸들(key handle)을 설정한다. 그리고 인증 장치는 생산 시에 설정된 증명 인증서(attestation certificate)용 개인키로 증명용 서명(attestation signature)을 생성한다. 그런 다음 인증 장치는 사용자 공개키, 키 핸들, 증명 인증서, 그리고 증명용 서명을 클라이언트를 통해 서버로 전송한다. 서버는 증명용 공개키를 사용하여 인증 장치의 증명용 서명을 검증하여 증명된 인증 장치가 맞음을 확인하고, 사용자 공개키를 키 핸들과 함께 해당 계정에 연결하여 저장한다.

4.3. 인증 절차

그림 5는 FIDO 인증 절차를 간략하게 보이고 있다. 특정 계정 사용자에 대한 인증이 필요한 서버는 인증 장치 수용 정책과 해당 계정에 미리 등록된 공개키에 대한 키 핸들, 그리고 서명 작성용 챌린지를 클라이언트를 통해 사용자가 선택한 인증 장치에 전송한다. 인증 장치 사용자는 미리 설정된 사용자 확인 방법(예, 지문인식)으로 사용자 인증을 수행하고, 키 핸들에 대응되는 사용자 서명용 개인키를 추출하여 사용자 인증용 서명을 생성한다. 그런 다음 서명은 클라이언트를 경유하여 서버로 전송되고, 서버는 해당 계정에 등록된 공개키를 사용하여 서명을 검증한다. 검증이 성공하면 서버는 인증 대상 사용자가 해당 계정에 공개키를 등록한 인증 장치를 소유하고 있음을 확인하게 되고, 이로써 사용자 인증을 대신하게 되는 것이다.

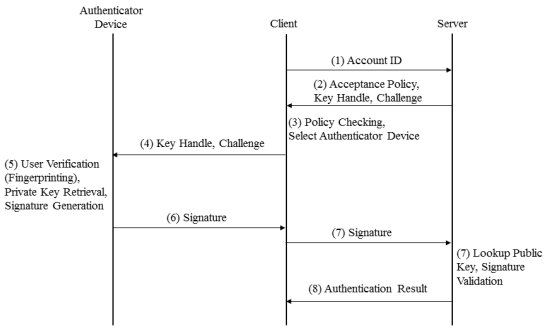

Fig. 5 FIDO User Authentication Procedure

개인에 대해 인증서를 발급하는 PKI 인증과 달리 FIDO 인증은 인증 장치의 보안 뿐만 아니라 처리 능력과 편의성을 고려하여 해당 생산자에 증명 인증서(attestation certificate)를 발급한다. 따라서 FIDO 인증은 인터넷 뱅킹과 같이 거래 내용을 사용자가 확인하고 거래 서명이 필요한 경우, 그림 6과 같이 수용 정책을 통해 사용자가 이에 합당한 인증 장치를 사용하게 하고, 안전한 인증 장치에 출력되는 거래 정보를 확인하고 안전하게 서명할 수 있도록 보장한다.

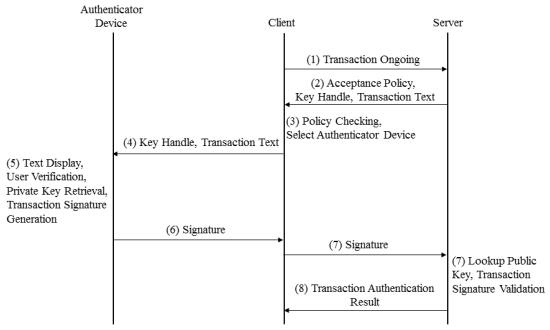

Fig. 6 FIDO Transaction Authentication Procedure

Ⅴ. 비 교

5.1. 인증서 발급

표 1은 PKI 인증과 FIDO 인증의 인증서 발급 측면의 차이를 요약하고 있다. PKI 인증을 위해 인증 대상이 되는 모든 사용자는 CA로부터 신원을 확인받고(identity proofing), 사용자의 공개키를 보증하는 인증서를 발급받아야 하고, 인증서를 유지하고 관리해야 한다. 반면

FIDO 인증에서는 개별 사용자는 인증서 발급과 유지. 관리에 전혀 참여할 필요가 없다. 즉, 사용자는 생산자가 자신이 생산하는 인증 장치의 능력에 대한 인증서를 발급 받은 후 생산하는 인증 장치를 단지 믿고 사용하기만 하면 된다. 따라서 인증서를 발급하고 관리하기 위한 인프라 구축비용 측면에서 보면, 사용자별 인증서 발급이 필요한 PKI 인증이 인증 장치 생산자별 인증서 발급이 필요한 FIDO 인증에 비해 높은 비용 구조를 가짐을 알 수 있다. 그리고 PKI 인증은 사용자가 인증서 발급, 유지, 그리고 관리에 직접 참여해야 하는 데 비해 FIDO 인증은 인증서와 관련하여 사용자의 참여가 불필요하므로, 사용자 편의성 측면에서 FIDO 인증이 유리함을 알 수 있다.

Table. 1 Comparison of Certification Aspect

Comparison Items	PKI Authentication	FIDO Authentication
certification subject	user	authenticator device maker
certification object	binding of identity and public key	capability of authentication device
user identity proofing	necessary	not necessary
infrastructure cost	high	low
user friendliness	low	high

5.2. 공개키 등록 및 적용 범위

표 2는 PKI 인증과 FIDO 인증의 공개키 등록 및 적용 범위에 대한 차이를 요약하고 있다. PKI 인증은 인증 서명을 검증하기 위한 공개키를 인증서 발급 시에 CA에 한번 등록하고, 인증서 유효 기간 동안 해당 공개키를 모든 PKI 사이트에서 서명 검증용으로 사용한다. 반면 FIDO 인증은 인증 장치에서 생성되는 공개키를 사용자가 접근하는 서버 별로 등록한다. 이 때 인증 장치가 생성하는 공개키는 서버마다 다르게 설정된다. 따라서 FIDO 인증에서 등록된 공개키의 적용 범위는 해당 서버에 한정되고, 동일 사용자가 동일 인증 장치를 통해 다른 서버에 제공하는 인증 서명을 검증하는 데에 사용할 수가 없다.

이는 서버들 간에 특정 사용자의 공개키를 공유할 수 없음을 의미하고, 따라서 해당 사용자가 각 서버에서 행한 행위를 연결하여 파악할 수 없게 됨으로써 사용자 프라이버시가 보장이 용이하다(unlinkability). 공개키 암호 프로토콜 기반의 서명은 특정 사용자의 거래 행위에 대한 부인 방지(non-repidiation)의 기본 수단이다. PKI 인증의 경우 사용자 공개키가 PKI 도메인의 모든 서버에서 해당 사용자의 서명 검증키 역할을 수행하므로, PKI 도메인 내의 모든 서버에 대해 부인 방지 서비스를 제공할 수 있다. 반면에 FIDO 인증의 경우 공개키의 적용 범위가 해당 공개키가 등록된 서버에 국한되므로, 부인 방지 서비스가 적용되는 범위도 해당 서버에 국한된다. FIDO 인증에서 사용자가 접근하고자 하는 모든 서버에 공개키를 등록해야 하는 절차는 사용자의 편의성을 낮추는 요인이 된다.

Table. 2 Comparison of Public Key Registration and Applicability Aspect

Comparison Items	PKI Authentication	FIDO Authentication
pubic key registration	CA	server
public key application scope	PKI domain	server domain
identity linkability	possible	impossible
non-repudiation applicability	PKI domain	server domain
privacy	low	high
user friendliness	high	low

5.3. 인증 및 개인키 보호

표 3은 PKI 인증과 FIDO 인증의 인증 방법 및 개인키 보호에 대한 차이를 요약하고 있다. PKI 인증은 사용자로 하여금 자신의 서명을 제시하게 하고, 제시된 서명을 검증함으로써 해당 사용자를 인증한다. 즉, BYOS (Bring Your Own Signature) 형식의 인증에 기초한다. 서명 검증은 인증서 발급 시에 설정된 개인키에 의한 서명 작성 여부만 확인할 뿐, 서명이 어디에서 생성되었는지는 고려하지 않는다. 따라서 PKI 개인키는 인증서 발급 시의 보호 체계를 준수하는 한 어디에나 저장될 수 있고, 따라서 서명 생성도 여러 곳에서 이루어질 수 있다.

반면 FIDO 인증의 경우 서명은 서버에 등록된 공개키를 생성한 인증 장치에 의해 반드시 생성되어야 하므로, 사용자는 반드시 해당 인증 장치를 소유하고 인증에 활용하는 BYOD(Bring Your Own Device) 형식의 인증에 기초한다. PKI 인증은 인증서의 신원 정보로 사

용자의 신원을 확인하는 반면, FIDO 인증은 서버에 등록한 공개키를 생성한 인증 장치를 해당 사용자가 소유하고 있음을 확인하는 측면에서도 차이가 있다.

Table. 3 Comparison of Authentication and Private Key Protection Aspect

Comparison Items	PKI Authentication	FIDO Authentication
authentication type	BYOS(Bring Your Own Signature)	BYOD(Bring Your Own Device)
authentication object	identity of user	presence of registered device
private key protection method	not certified (password)	certified (biometrics)
private key container	not certified (HDD/USB)	certified (authenticator device)
signature generation place	not certified (client)	certified (authenticator device)
flexibility	high	low
security	low	high
user friendliness	low	high

PKI 인증에서 개인키 보호 방법은 표준화되어 있지 않고, 인증서 기반 서비스 제공자의 선택 사항이다. PKI 인증 서비스 제공자들은 자신의 서비스 요구사항에 맞는 개인키 보호 방법을 구현하여 사용자들에게 제공하고 있다. 일반적인 보호 방법은 패스워드 기반의 암호키를 사용하여 개인키를 암호화하여 보호하며, 저장 장소는 사용자 편의성과 비용 등을 고려하여 HDD 또는 USB 메모리를 사용하고 있다. 반면 FIDO 인증은 개인키 저장과 보호 방법, 그리고 안전한 서명 생성 과정 등이 인증 장치 생산자에 대한 증명 인증서 발급 과정의 증명 사항이다. 따라서 FIDO 인증 기반 서비스 제공자는 자신의 서비스에 적합한 인증 장치를 믿고 선택하여 서비스를 제공할 수 있다. FIDO 인증 장치는 개인키 보호를 위해 신뢰 플랫폼(trusted platform) 기반의 저장과 생체인식 인증(biometrics authentication)을 통해 안전성과 편리성을 보장하고 있다. 뿐만 아니라 FIDO 인증의 경우 서명 생성이 신뢰 플랫폼인 인증 장치에서 생성되도록 보장함으로써, 웹 브라우저나 범용 OS의 응용에서 서명이 생성되는 경우 메모리상에서 공격자에 의해 서명 대상 내용이 위조되는 MITB(Man In The Browser) 공격[18] 등을 방어할 수 있다. 즉, 서명의 안전성을 보장할 수가 있다.

반면 FIDO 인증은 어떤 경우에도 서버에 등록된 인증 장치를 반드시 사용해야 한다는 측면에서 유연성이 떨어지는 문제가 있다.

5.4. 응용

앞에서 살펴본 것처럼 PKI 인증과 FIDO 인증은 공개키 암호 프로토콜에 기초하지만, 분명한 차이로 인해 적합한 응용 분야가 다른 수밖에 없다. 표 4는 응용 측면에서 PKI 인증과 FIDO 인증을 비교하고 있다.

Table. 4 Comparison of Application Aspect

Comparison Items	PKI Authentication	FIDO Authentication
identity proofing applications(civil application services, federal employee identification)	>	
identity pre-proofed applications(payment gateway, internet banking)	<	
platform-flexible applications	>	
smartphone-based Applications	<	
peer-to-peer applications	>	
strong-security applications	<	

A > B : A better than B

PKI 인증의 경우 사용자 개개인이 신원 확인 후 발급된 인증서를 가지고 있으므로, 실시간으로 사용자 신원 확인이 필요한 응용에 적합하다. 예를 들어, 사용자는 정부의 모든 민원 서비스 사이트에 인증서와 서명을 제시함으로써, 자신의 신원을 확인받고 필요한 민원 서비스를 제공받을 수 있다. 연방 정부의 직원이 정부의 각 기관으로부터 자신의 신원을 확인받을 때도 PKI 인증을 응용할 수 있다. 만약 이런 응용에 FIDO 인증을 응용하고자 한다면, 사용자는 각 사이트에 자신의 신원 확인 후 계정을 개설해야 하고, 해당 계정에 FIDO 인증 장치를 등록하는 절차를 거쳐야하기 때문에 불편할 수밖에 없다. 정부 기관의 경우 직원 또는 민원인을 대상으로 인증서를 발급하고 관리하는 인프라 구축이 비교적 용이한 점도 PKI 인증 응용이 적합한 이유이다.

서비스 특성상 해당 서비스를 제공하기 위해 반드시 사전에 사용자 신원 확인과 계정 개설 작업이 선행되어

야 하는 경우가 많다. 쇼핑몰 등에 결제 대행 서비스를 제공하는 PG(Payment Gateway)의 경우, 결제 계좌 또는 결제 카드 등록을 위한 사전 신원 확인과 그에 따른 적절한 등록 과정을 거쳐야 한다. 인터넷 뱅킹의 경우에도 계좌 개설 과정에서 사용자에 대한 신원 확인 과정을 반드시 거치게 된다.

따라서 이런 응용의 사용자 인증의 경우, 사용자에 대한 추가적인 신원 확인 보다 등록된 사용자 여부를 안전하고 편리하게 확인하는 것이 중요하므로, 인증서 발급 및 관리 인프라가 필요한 PKI 인증 보다, 자체적인 신원 확인 과정에서 인증 장치 등록만 하면 되는 FIDO 인증이 적합함을 알 수 있다. 만약 우리나라와 같이 모든 은행과 PG들이 공통적으로 사용할 수 있는 PKI 인프라가 잘 구축되어 있고, 인증서와 개인키 보호 메카니즘이 FIDO 인증 장치와 같이 안전하고 편리하게 제공된다면, PKI 인증도 이와 같은 응용에 여전히 좋은 대안이 될 수 있다.

FIDO 인증 장치는 생체인식 기반의 인증 기술과 신뢰 플랫폼 기반의 개인키 보호와 서명 생성을 요구한다. 따라서 FIDO 인증이 적용되는 환경은 최신 사양의 스마트폰과 같은 특별한 플랫폼에 국한될 수밖에 없다. 반면에 PKI 인증은 생체인식 기능이나 신뢰 플랫폼 기술이 적용되지 않은 기존 PC와 같은 다양한 플랫폼에서도 유연하게 응용될 수 있는 장점이 있다. FIDO 인증은 서버에 인증 장치의 공개키를 사전 등록하는 절차를 반드시 거쳐야 한다. 따라서 P2P(Peer to Peer) 응용과 같이 많은 수의 장치들 간에 상호 인증이 필요한 경우에는 등록 절차 수행에 따른 부담이 커서 FIDO 인증을 적용하기가 어렵다. FIDO 인증의 가장 큰 장점은 개인키 보호와 서명 생성이 안전성이 보장된 인증 장치에서 이루어지는 것이다. FIDO 인증을 적용하면 현재의 PKI 인증에서 문제가 되고 있는 피싱 및 파밍 공격, 악성 소프트웨어에 의한 개인키 복제 및 패스워드 도청 공격, MITB 공격 등을 방어할 수 있다. 강한 보안성을 요구하는 응용에는 PKI 인증 보다 FIDO 인증이 바람직하다. PKI 인증을 FIDO 인증과 같은 수준의 강한 보안 응용에 적용하기 위해서는 개인키 보호 및 서명 생성 메카니즘을 FIDO 인증 장치 수준으로 높일 필요가 있다.

Ⅵ. 결 론

PKI 인증은 공개키 암호 프로토콜을 사용하여 개인키 소지와 패스워드 지식의 2 요소의 강력한 인증을 서비스를 제공함으로써, 우리나라를 중심으로 인터넷 뱅킹 등 안전이 매우 중요한 인터넷 거래에 활발하게 사용되어 왔다.

그러나 인증서 인프라 구축 비용, 인증서 관리 부담에 따른 사용자 불편, 패스워드 기반의 개인키 보호에 따른 안전성과 사용자 불편 문제 등으로 새로운 대안 개발도 활발하게 진행되어 왔다. 본 논문은 결제 대행 서비스와 인터넷 뱅킹 등의 분야에서 PKI 인증의 대안으로 떠오르고 있는 FIDO 인증을 기존 PKI 인증과 비교 분석하였다. 생체인식과 결합된 FIDO 인증은 자주 접근하는 서버에 인증 장치를 한번 등록하고 나면, 인증서 관리가 불필요하고 패스워드에 비해 높은 관리 편의성과 안전성을 지원한다.

따라서 이러한 특성에 부합하는 인터넷 뱅킹과 결제 대행 서비스 등을 인증 장치로 사용가능한 스마트폰으로 제공하는 경우, FIDO 인증은 더 큰 주목을 받을 것으로 예상된다. 그러나 FIDO 인증은 일정 수준 이상의 보안 능력이 갖추어진 인증 장치에서만 제공이 가능하고, 서버별로 별도의 등록 절차가 필요하며, 공개키의 응용 범위가 등록 서버에 국한되는 등 기존의 PKI 인증과 다른 특징들로 인해, PKI 응용을 빠른 시일 내 광범위하게 대체하기는 어려울 것으로 전망된다. 대신 향후 상당 기간 동안 PKI 인증과 FIDO 인증은 상호 경쟁하며 공존하는 것이 불가피할 것이다.

따라서 우리나라와 같이 PKI 인증이 활성화되어 있는 경우 PKI 인증과 FIDO 인증을 절절하게 응용하는 것은 효과적인 인터넷 안전 거래 인프라 구축에 매우 중요하다. 기존의 인프라를 활용할 수 있는 PKI 인증이 효과적인 응용에 FIDO 인증을 신규로 적용하는 것은 낭비를 초래할 것이다. 반면, FIDO 인증을 통해 보다 안전하고 편리한 서비스를 제공할 수 있는 응용에 기존 PKI 인증을 계속 적용하는 것은 인터넷 거래 활성화의 걸림돌이 될 것이다. 본 연구가 PKI 인증과 FIDO 인증을 적절하게 활용하여 향후 인터넷 안전 거래 인프라를 효과적으로 발전시켜가는 데에 작은 초석이 되기를 기대한다.

ACKNOWLEDGMENTS

This paper was studied by the support of education and research promotion program for professors of Korea University of Technology and Education

REFERENCES

[1] Korea Internet & Security Agency. 2016 National Information Security White Paper[Internet]. Avaliable : http://isis.kisa.or.kr/ebook/download_pdf/.

[2] FIPS PUB 201-2, *Personal Identity of Verification(PIV) of Federal Employees and Contractors*, National Institute of Standards and Technology, August 2013.

[3] FSA 2010-001, *A Management Guide for Financial Part Encryption Technologies*, Financial Security Agency, Jan. 2010.

[4] Y. K. Song, "Lessons of Public Certificate-related Debates and A Policy-direction Proposal for Future Digital Transactions," *KDI FOCUS*, No. 51, pp. 1-8, March 2015.

[5] J. H. Lee, "Usability of Accredited Certificate and Its Problems in Smart Environments," *Internet & Security Focus*, pp. 23-53, March 2013.

[6] H. S. Kim, J. H. Huh, and R. Anderson, "On the Security of Internet Banking in South Korea," Oxford Univ. Computing Laboratory, Technical Report CS-RR-10-01, Oct. 2010.

[7] S. W. Chai, K. S. Min, and J. H. Lee, "A Study of Issues about Accredited Certification Methods in Korea," *International Journal of Security and Its Applications*, vol. 9, no. 3, pp. 77-84, March 2015.

[8] FIDO Alliance, Specifications Overview [Internet]. Avaliable : https://fidoalliance.org.

[9] RFC 5246, *The Transport Layer Security(TLS) Protocol Version 1.2*, IETF, Aug. 2008.

[10] S. C. Park, "A Comparative Analysis of NPKI and SSL/PLS for Secure Internet Transactions," *Journal of the Korea Institute of Information and Communication Engineering*, vol 20, no. 2, pp. 289-298, Feb. 2016.

[11] KISA, "Research on the Actual Condition of Electronic Signature System Usage," Technical Report KISA-WP-2015-0032, Dec. 2015.

[12] A. Hiltgen, T. Kramp, and T. Weigold, "Secure Internet Banking Authentication," *IEEE Security & Privacy*, pp. 21-29, March/April 2006.

[13] FIDO Alliance, Universal 2nd Factor(U2F) Overview [Internet]. Avaliable : https://fidoalliance.org.

[14] FIDO Alliance, FIDO UAF Architectural Overview [Internet]. Avaliable : https://fidoalliance.org.

[15] FIDO Alliance, Response to NIST RFI on the Framework for Improving Critical Infrastructure Cybersecurity [Internet]. Avaliable : http://csrc.nist.gov/cyberframework/rfi_comments_02_2016/.

[16] Korea JoongAng Daily, Hana to Use Biometrics to Make Internet Banking Safer[Internet]. Avaliable : http://koreajoongangdaily.joins.com/news/article/.

[17] RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, May 2008.

[18] Y. J. Maeng, D. O. Shin, S. H. Kim, D. H. Nyang, and M. K. Lee, "A Vulnerability Analysis of MITB in Online Banking Transactions in Korea," *Internet and Information Security*, vol 1, no. 2, pp. 101-118, Nov. 2010.

박승철(Seungchul Park)

1985.2 : 서울대 계산통계학과 졸
1987.2 : KAIST 전산학과 석사
1996.8 : 서울대 컴퓨터공학과 박사
ETRI 연구원, 한국IBM, 현대전자 네트워크연구소장, 현대네트웍스(주) 연구소장 역임,
현재 한국기술교육대학교 컴퓨터공학부 교수
※관심분야 : 컴퓨터 네트워크, 네트워크 보안, 핀테크 보안