https://doi.org/10.14400/JDC.2017.15.8.183

FIDO 생체기술과 안전영역을 연계한 공인인증서 효율화 방법

조화건*, 양해술**
금융결제원 정보보호본부*, 호서대학교 벤처대학원 교수**

A Methodology for the Improvement of Accredited Digital Certificate Integrating FIDO Biometric Technology and TrustZone

Hwa-Gun Cho*, Hae-Sool Yang**
Information Security Group, Korea Financial Telecommunications & Clearings Institute*
Graduate School of Venture, Hoseo University, Professor**

요 약 전자서명법에 따라 발급되고 있는 공인인증서는 비대면 거래에서의 필수 기능을 제공하기 때문에 전자금융거래, 전자민원 등 다양한 분야에 이용되고 있다. 하지만 공인인증서는 파일로 저장할 경우 해커로 인한 유출이 가능하며 이용 시 별도 프로그램 설치가 필요하기 때문에 안전성, 편리성 양 측면에서 비판을 받고 있다. 최근 패스워드 기반 인증의 문제점과 인증수단 간 부족한 상호 운용성을 해결하려는 시도로 등장한 FIDO가 생체기술 기반 인증에서 이용되고 있으며, 하드웨어 기반 보안 운영환경인 안전영역이 안전한 스마트폰 이용을 위해 활용되고 있다. 본 고에서는 공인인증서의 문제를 해결하기 위해 FIDO를 이용하여 생체기술 인증을 수행하고 공인인증서는 안전영역에 저장하도록 하는 새로운 형태의 공인인증서 이용 방식을 제시하였다. 제시된 방식은 기존 방식에 비해 안전성과 편리성을 향상시켰을 뿐 아니라 최신 스마트폰에 기본 탑재된 생체정보 인식기능과 안전영역을 이용하였기 때문에 서비스의 적용이 용이하다는 장점이 있다. 이 방식으로 공인인증서 이용이 더 안전하고 편리해지리라 기대해 본다.

주제어 : 공인인증서, FIDO, 생체기술, 안전영역, 모바일 보안

Abstract Digital accredited certificates issued under the Digital Signature Act provide essential functionalities for online service, so certificates are used for various services such as online banking, e-government. However, certificates can be stolen by hackers and users need to install separate software to use certificates. Recently FIDO, which aims to solve the problems of password-based authentication and the lack of interoperability between authentication methods, is used for biometric authentication and TrustZone, hardware-based secure environment, is used for safe smartphone usage. In this paper, the new service method is suggested which uses FIDO-based biometric authentication and stores certificates in TrustZone. This method can not only improve security and convenience but also be easily applied to the service because it uses built-in functionalities of new smartphones such as biometric sensors and TrustZone. It is expected that people can use certificates in a safe and convenient way with this method.

Key Words : Accredited Digital Certificate, FIDO, Biometric Technology, TrustZone, Mobile Security

Received 21 June 2017, Revised 27 July 2017
Accepted 20 August 2017, Published 28 August 2017
Corresponding Author: Hae-Sool Yang
(Graduate School of Venture, Hoseo University)
Email: hsyang@hoseo.edu

ISSN: 1738-1916

1. 서론

정보통신기술의 발전과 정보통신망 확산은 상거래에도 커다란 변화를 가져왔는데 우리는 시간을 절약하고 이동에 따른 번거로움 등을 피하기 위해 정보통신망으로 연결된 비대면 거래인 전자상거래를 이용하는 것을 당연시하고 있다. 비대면 거래에서는 신원확인 곤란, 거래사실의 부인, 거래의 위·변조 가능성 등의 문제가 발생된다. 이에 따라 정부에서는 비대면 거래의 전자상거래는 물론, 모든 전자거래에서 안심하고 사용할 수 있는 온라인 인감증명서를 만들었는데 이를 공인인증서라 한다. 즉 인증서란 서명이나 인감도장과 같은 역할을 하는 전자서명이 특정인에게 유일하게 속한다는 사실을 확인하고 이를 증명하는 전자적 정보를 말하며, 공인인증기관이 발급하는 인증서를 공인인증서라 한다. 따라서 공인인증서는 거래당사자의 신분확인은 물론 거래의 위·변조 방지 및 거래 사실의 부인방지 등의 기능을 가지고 있어 안전한 전자거래를 보장한다.

2003년 정부에서 시행한 전자금융거래에서의 공인인증서 의무사용으로 금융권의 인터넷뱅킹에 공인인증서를 사용함에 따라 급격히 공인인증서의 발급이 증가되었고 다양한 분야에서 공인인증서가 사용되었다. 2016년을 기준으로 공인인증서는 3,000만 건 이상 발급되어 이제는 우리 일상생활에서 없어서는 안 되는 공공재가 되었다.

하지만 해커들의 해킹기술 또한 빠른 속도로 발전하여 네트워크 및 악성코드를 통해 개인 컴퓨터 하드디스크에 존재하는 공인인증서가 유출(2015년;22,796건, 2016년 6월;6,815건)되어 전자금융사고로 이어지고 있으며 특정 웹브라우저에 적용한 액티브X가 사용자 이용에 불편함을 주는 문제가 발생되고 있다. 또한 안전성을 강조하다 보니 공인인증서 발급 및 갱신은 물론 타행에 등록할 경우 사용자의 편리성이 부족한 형편이다. 아울러 정부에서는 다양한 인증수단 사용을 권장하기 위해서 2015년부터 전자금융거래에서의 공인인증서 의무사용을 폐지하였다.

한편 금융권에서는 생체인증을 이용한 본인인증수단 개발, IC카드를 이용한 인증수단 등을 개발하여 적용하고 있으며, 공인인증기관 및 한국인터넷진흥원(KISA)에서도 공인인증서에 대한 편의성제고 방안 등을 강구하고 있다.

이러한 상황에도 공인인증서는 금융부문의 인터넷뱅킹뿐 아니라 간편한 연말정산, 전자입찰, 쇼핑몰, 학사업무 등 다양한 분야에서 사용되고 있어 공인인증서의 사용은 지속될 것으로 전망된다.

이에 본 고에서는 공인인증서의 문제점으로 지적되고 있는 공인인증서의 유출과 편의성의 문제를 FIDO기반 생체기술과 안전영역(TrustZone)을 연계하여 효율성을 강화할 수 있는 방법을 제안하고자 한다. 2장에서는 공인인증서 및 공인인증서와 연계하려는 FIDO 생체기술과 안전영역에 대한 기술을 살펴보고 3장에서는 공인인증서와 관련한 이슈에 대해 분석하고자 한다. 마지막으로 4장에서는 분석한 내용을 바탕으로 FIDO 기반의 생체기술과 안전영역을 연계한 공인인증서의 효율성 강화 방안을 제안하고 5장에서는 본 연구에 대한 요약과 결론을 제시하고자 한다.

2. 공인인증서 및 연계 기술

2.1 공인인증서

비대면 거래에서의 필수 기능인 ① 서비스에 접근하려는 사람의 신원을 확인하는 인증(Authentication), ② 서비스에 접근하려는 사람이 권한 있는 사람인지 확인하는 인가(Authorization), ③ 암호화를 통해 외부에서 정보를 가독할 수 없도록 하는 기밀성(Confidentiality), ④ 전송되는 데이터가 외부에 의해 변조되지 않도록 하는 무결성(Integrity), ⑤ 송신자가 데이터 송신사실을 부인하지 못 하도록 하는 부인봉쇄(Non-repudiation)의 5대 기능을 가진 PKI(Public Key Infrastructure)를 기반으로 하는 공인인증서를 만들기 위해 정부 정보보호분과위원회와 정보통신부(현 미래창조과학부)는 「PKI 구축 및 운영에 관한 기본정책 」을 수립하고 <Table 1>과 같이 관련 알고리즘 및 표준규격을 발표함과 더불어 미국보다 앞서 전자서명법이 1999. 7. 1. 시행하면서 국내에서는 공인인증서가 발급되었다.

<Table 1> Algorithms and Standard

□ Digital Signature Algorithm - KCDSA(TTA Standard)
□ Hash Algorithm - HASH-160(TTA Standard) - SHA-1(FIPS 180-1)
□ Distinguished Name - ITU-T X.520(International Standard)
□ Object IDentifier - ISO(International Standard)

□ Digital Certificate - ITU-T X.509(Internation Standard) 1. Certificate Profile: IETF RFC 2459 2. Certificate Management: IETF RFC 2510, 2511 3. Certificate Access: IETF RFC 2559 4. Certificate Revocation and Status Retrieval: IETF RFC 2560 5. Timestamp Service: ISO/IEC 18014 PART 1~3 6. Policy and Certification Practices Framework: IETF RFC 2527

공인인증서는 공개키 암호방식의 전자서명이 기반이 된다. 공개키 암호방식이란 암호화할 때 사용하는 키와 복호화할 때 사용하는 키를 별도로 사용하는 방식으로 상대방에게 공개하는 공개키(Public Key)로 암호화한 암호문은 키를 생성한 자신이 비밀로 유지하고 있는 개인키(Private Key)로만 해독이 가능하고 역으로 개인키로 암호화한 암호문은 공개키로만 해독이 가능하도록 구현함으로써 비밀키 암호방식의 키 분배 및 부인봉쇄 문제를 해결한 암호방식을 말한다[1]. 따라서 전자서명이라 함은 공개키 암호방식에서 개인키를 이용한 메시지 암호화는 서명 당사자 밖에 할 수 없다는 점을 이용하여 구현한 것으로 서명자를 확인하고 서명자가 당해 전자문서에 서명하였음을 나타내는데 이용하기 위하여 당해 전자문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보를 말한다(전자서명법 제2조 제2호)[2].

국내에서 전자거래 사실을 공정하게 관리 및 보증할 수 있는 공신력과 인증시스템을 구축하고 관리할 수 있는 전문 인력과 기술력, 재무건전성을 갖춘 기관으로 전자서명법 제4조에 따라 미래창조과학부 장관이 지정한 기관을 공인인증기관이라 하며 공인인증기관이 전자서명법 제15조에 따라 발급한 것을 공인인증서라 한다. 국내에는 금융결제원(금융 2000. 4. 12), 코스콤(증권 2000. 2. 10), ㈜한국정보인증(일반 2001. 11. 24), ㈜한국무역정보통신(전자무역 2002. 3. 11) 5개 기관의 공인인증기관이 있으며 발급되는 공인인증서는 개인과 법인 그리고 단체에게 발급되며 모든 전자거래에서 사용할 수 있는 유료인 범용 공인인증서와 은행, 신용, 보험, 정부 민원에서만 사용되는 무료인 용도제한용 공인인증서가 있다[3].

공인인증서에는 <Table 2>와 같은 내용이 포함되며[4,5] 국내의 공인인증업무체계를 살펴보면 전자서명 및 인증업무 관련 정책의 수립 및 시행과 함께 감독을 관장하는 미래창조과학부가 있고 최상위인증기관(Root CA)으로 한국인터넷진흥원(KISA)이 있으며 공인인증기관(Certification Authority)과 함께 등록(대행)기관(Registration Authority)으로 이루어져 있다.

<Table 2> Digital Certificate Profile

Basic Field	{Version ‖ Serial Number ‖ Signature Algorithm ‖ Issuer ‖ Validity ‖ Subject ‖ Subject Public Key Info}
Extension Field	{Authority Key Identifier ‖ Subject Key Identifier ‖ Key Usage ‖ Certificate Policies ‖ Policy Mapping ‖ Subject Alternative Name ‖ Issuer Alternative Name ‖ Basic Constraints ‖ Name Constraints ‖ Policy Constraints ‖ Extended Key Usage ‖ CRL Distribution Points ‖ Authority Information Access}
Certificate Authority Signature	

마지막으로 국내의 금융기관에서 발급되는 공인인증서의 처리흐름을 살펴보면 가입자는 사전작업으로 은행 지점을 방문하여 대면으로 신원을 확인하고 인터넷뱅킹에 가입한다. 은행은 공인인증기관 인증서생성관리시스템으로 인증서 신청자를 등록하고 인증기관에서는 등록이 완료됨을 알리는 인가코드를 은행으로 보낸다. 은행은 가입자에게 이를 통지하면 가입자 컴퓨터에서는 키쌍 및 인증서 발급요청 메시지를 생성하여 직접 공인인증기관에 인증서 발급을 요청한다. 공인인증기관은 공인인증서를 발급하여 가입자에게 전송함으로서 발급이 완료되고 가입자는 이를 이용하게 된다.

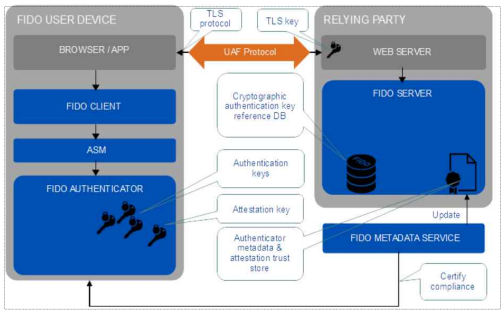
2.2 FIDO 기반 인증기술

최근 핀테크 확산과 더불어 패스워드, 공인인증서 등 기존 인증수단을 보완하거나 대체하려는 시도가 늘고 있음에 따라 2013년 2월에 IT업체 및 카드사, 글로벌 전자회사를 중심으로 비영리 사단법인인 FIDO(Fast IDentity Online) Alliance를 설립하여 온라인 환경에서 주로 이용되는 패스워드 기반의 인증의 문제점과 다양한 인증수단

사이의 부족한 상호 운용성을 해결하는 시도가 시작되었다[6,7,8].

FIDO Alliance에서는 두 가지에 대해 표준화를 하였는데 첫 번째가 온라인 서비스에서 사용하던 패스워드 인증(서버에서 인증)을 사용자의 디바이스에서 인증으로 대신하는 「범용 인증 프레임워크 프로토콜(Universal Authentication Framework Protocol)」이고 두 번째가 기존 패스워드 기반 인증과 더불어 USB 등의 별도 기기를 이용해 추가 인증하는 「U2F 프로토콜(Universal 2nd Factor Protocol)」이다[9].

첫 번째인 UAF 프로토콜은 기존 패스워드 기반 인증의 단점인 사용자 인증정보를 중앙서버에 보관함으로써 발생되는 인증정보의 대량 탈취의 위험성 상존, 피싱 공격에 대해 취약, 스마트폰에서의 사용 불편, 서비스마다 다르게 사용하는 패스워드 관리의 어려움 등을 극복하기 위해 고안되었다. 이 프로토콜은 인증과정을 로컬인증과 원격인증으로 구분하는 특징을 가지고 있다. 로컬인증은 사용자 디바이스에서 지문, 홍채, 정맥 등의 생체정보 혹은 PIN을 이용하여 사용자 확인(User Verification)을 하는 것을 말한다. 원격인증은 공인인증서에서의 기반이 되는 공개키 암호화 방식의 전자서명을 활용해 기존에 등록된 디바이스인지를 검증하는 방식을 말한다.



(fidoalliance.org)

[Fig. 1] FIDO High-Level Architecture

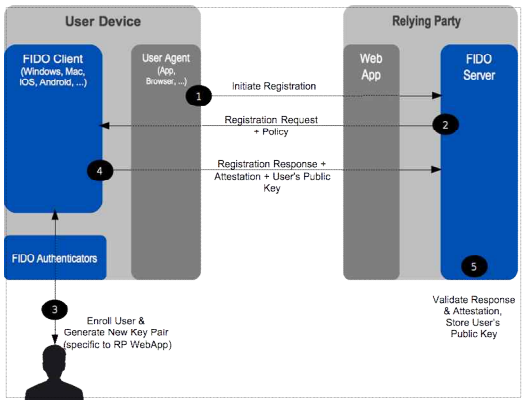
UAF 프로토콜의 구성요소를 살펴보면 [Fig. 1]과 같이 사용자 확인을 수행하는 사용자 디바이스와 서비스 제공 및 인증을 담당하는 서버로 구분된다. 사용자 디바이스에서는 생체인증, PIN 등을 이용해 사용자 확인을 거쳐 전자서명 값을 서버에 전송하며 서버에서는 사용자 디바이스에서 보내온 전자서명 값을 검증하게 된다.

사용자 디바이스는 FIDO Client, ASM(Authenticator Specific Module), FIDO Authenticator, Authentication Key, Attestation Key로 구성되어 있다.

FIDO Client는 사용자 디바이스에서 UAF 혹은 U2F 프로토콜 메시지를 해석하는 소프트웨어이다. ASM은 FIDO Client가 표준화된 형태로 FIDO Authenticator에서 사용할 수 있도록 제공하는 인터페이스이다. FIDO Authenticator는 사용자 확인 및 그와 관련된 암호화 연산과정을 수행하는 연산장치로서 홍채, 정맥, 지문 PIN 등 여러 인증수단이 가능하며 기기에 내장되어 있거나 USB나 블루투스 등 별도의 장치가 될 수 있다.

Authentication Key는 서버에 등록할 때 생성되는 사용자의 개인키이다. Attestation Key는 Authenticator제조시점에 내장되어 있는 개인키로 최초 FIDO 등록 시에 생성하는 사용자의 공개키를 서버에 보낼 때에 전자서명을 하기 위한 용도로 사용한다.

서버는 FIDO 서버와 Authenticator Metadata로 구성되어 있다. FIDO 서버는 FIDO 클라이언트가 프로토콜에 의해 보내온 메시지를 해석하여 등록, 인증, 거래확인, 해지 등의 기능을 수행한다. Authenticator Metadata는 Authenticator의 특성을 나타내는 Authenticator의 버전, Authenticator ID, Authenticator 루트 인증서, 사용자 확인수단(지문, 음성, 얼굴, 홍채 등), 키 보호유형(소프트웨어, 하드웨어 등), 전자서명 알고리즘 및 인코딩 방식 등의 정보를 가지고 있다. Authenticator 제조사는 메타 데이터 정보를 FIDO Alliance에서 운영하는 MDS(Metadata Service)를 통하거나 혹은 직접 제공할 수 있다.



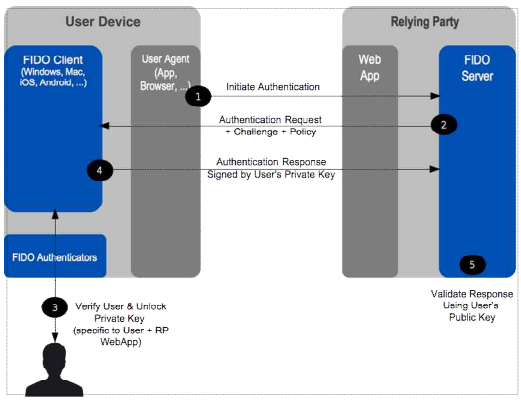
(fidoalliance.org)

[Fig. 2] FIDO Registration Message Flow

UAF 프로토콜의 흐름을 살펴보면 먼저 [Fig. 2]와 같이 사용자의 공개키를 FIDO 서버에 등록한다.

① 서버에 로그인 및 FIDO 인증 등록 요청
② 서버는 등록 가능한 Authenticator 정보를 담은 정책과 임의의 Challenge값 등을 포함한 등록 요청 메시지를 전송
③ FIDO 클라이언트는 서버가 보내온 정책을 바탕으로 기기에서 사용 가능한 Authenticator를 조회 후 사용자에게 제시. 사용자는 Authenticator를 선택하고 생체인증정보 등을 기기에 입력하면 Authenticator는 공개키-개인키 쌍을 생성
④ 생성한 공개키 등을 담은 응답 값을 Attestation Key로 전자서명하여 서버로 전송
⑤ 서버는 응답 메시지를 검증하고 사용자의 공개키를 저장

그 다음에는 등록과정을 거친 Authenticator를 이용해 사용자를 [Fig. 3]과 같이 인증한다.

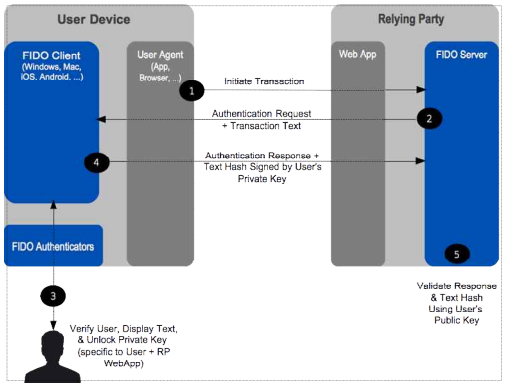


(fidoalliance.org)

[Fig. 3] FIDO Authentication Message Flow

① 서버에 FIDO 인증 요청
② 서버는 인증 가능한 Authenticator 목록을 담은 정책과 Challenge값 등을 포함한 인증 요청 메시지 전송
③ 사용자는 사전에 등록한 Authenticator를 이용해 인증을 수행
④ Challenge값 등을 포함한 데이터를 사용자 개인키로 전자서명을 해서 서버로 전송
⑤ 서버는 등록된 공개키로 클라이언트가 전송한 전자서명 데이터를 검증

그리고 요청메시지에 거래내용을 추가해 [Fig. 4]와 같이 사용자가 확인 후 인증을 수행하는 거래 확인을 한다.

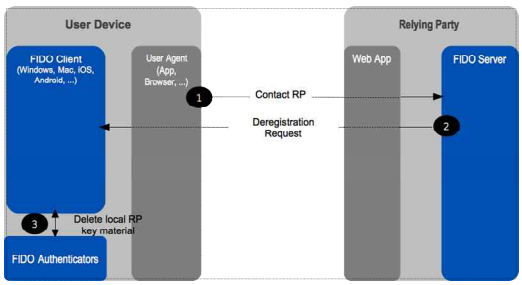


(fidoalliance.org)

[Fig. 4] FIDO Confirmation Message Flow

① 서버에 거래 시작 요청
② 서버는 정책, Challenge값, 거래 내용을 담은 인증 요청 메시지 전송
③ 사용자는 거래내용 확인 및 사전에 등록한 Authenticator를 이용해 인증을 수행
④ Challenge값, 거래 내용 등을 포함한 데이터를 사용자 개인키로 전자서명을 해서 서버로 전송
⑤ 서버는 등록된 공개키로 클라이언트가 전송한 전자서명 데이터를 검증

또한 클라이언트와 서버에 저장된 FIDO 관련 계정정보 등을 [Fig. 5]와 같이 삭제하는 기능을 정의하고 있다.

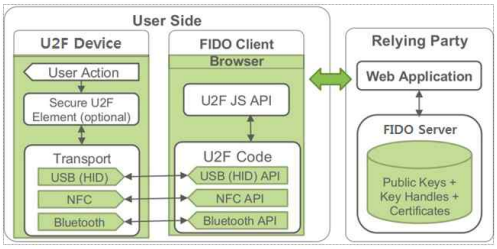


(fidoalliance.org)

[Fig. 5] FIDO Deregistration Message Flow

① 서버에 접속
② 삭제할 Authenticator 정보를 담은 해지 요청 메시지 전송
③ 클라이언트는 저장된 키 정보 삭제

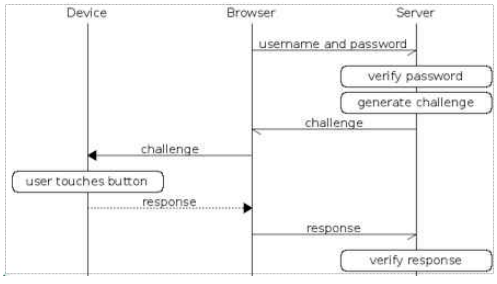
두 번째의 U2F 프로토콜은 패스워드 기반의 1차 인증을 수행한 뒤에 소지하고 있는 별도의 장치를 이용해 2차 인증을 수행하는 방식을 말한다. UAF 프로토콜과 마찬가지로 전자서명 방식을 활용하며 개인키가 U2F 디바이스(UAF의 Authenticator 역할을 수행하며 USB, NFC, 블루투스 등을 이용)내의 안전영역에 저장된다. U2F의 구성은 [Fig. 6]와 같이 구성되어 있다.



(wso2.com)

[Fig. 6] U2F Architecture

U2F 디바이스는 키를 생성하고 저장하며 암호화하는 연산과정을 수행하는 장치이다. FIDO 클라이언트는 U2F 프로토콜 메시지를 해석하는 소프트웨어로서 일반적으로 브라우저에 해당한다. FIDO서버는 FIDO클라이언트가 보내온 프로토콜 메시지를 해석하여 [Fig. 7]과 같이 등록과 인증을 수행하며 U2F 디바이스에서 생성한 공개키를 저장한다.



(www.yubico.com)

[Fig. 7] U2F Process Flow

현재 구글, 드롭박스 등의 웹사이트에서 U2F 인증을 지원하고 있다.

2.3 스마트폰에서의 안전영역 기술

국내에서 스마트폰에 공인인증서를 저장하여 본인인증수단으로 이용하게 된 것은 2008년 국민은행이 국내 최초로 공인인증서 기반의 칩 없는 모바일 뱅킹(인터넷 뱅킹용 프로그램을 이동통신기기에 다운로드하여 이용하는 VM(Virtual Machine)방식이며 칩 기반의 모바일 뱅킹과 구분하여 칩 없는 모바일 뱅킹이라 불림) 서비스를 실시하면서 피처폰에 저장된 공인인증서를 직접 호출하여 전자거래에 이용하면서부터 시작되었으며 스마트폰의 기술 발전과 함께 대부분 스마트폰을 이용함에 따라 공인인증서 사용은 자연스러운 일상이 되었다[10].

2010년 4월 스마트폰에서 국내 최초의 악성코드(국제전화를 무단으로 발신하여 과금 피해를 유발시키는 WinCE/Terdial악성코드)가 발견된 후 피싱, 파밍, 스미싱 등을 유발하는 모바일 악성코드의 발생건수가 증가하고 있고 최근에는 악성코드 제작도구(SpyEye 등)의 배포, 시스템 레벨에서의 해킹 기술이 지능화되면서 스마트폰에 악성코드를 감염시켜 앱을 위조 또는 변조하거나 보안 프로그램을 무력화하여 결제에 관련한 인증정보를 유출하는 사례가 증가하고 있어 미래창조과학부 산하기관이 한국인터넷진흥원에서는 공인인증서 유출을 완전 차단하는 스마트인증을 2013년 9월에 도입하였다. 이와 함께 업계에서도 다양한 보안 대응기술을 발표하는데 이 중 관심을 끄는 것이 바로 하드웨어 기반기술 중 TEE(Trusted Environment Execution) 기술로서[11] 모바일 단말에서 안전영역(TrustZone)기반의 하드웨어 칩을 이용하여 서비스의 안전한 실행을 보장하기 위한 보안 운영환경(Secure OS)을 제공하는 기술이다[12,13]. 여기에서 안전영역이란 하드웨어와 소프트웨어가 결합된 보안을 위해서 ARM사가 AP(Application Processor)내에서 제공하는 하드웨어 기능을 말하며 물리적으로 일반영역과 보안영역이 분리되어 있어 보안을 필요로 하는 공인인증서, 데이터 등을 보안영역에 저장할 수도 있고 응용프로그램 등을 보안영역에 저장하여 실행함으로써 해킹으로부터 안전하게 보호할 수 있다[14].

3. 공인인증서와 관련한 이슈

3.1 공인인증서 파일 유출

비대면 전자거래에서 본인임을 확인하기 위해 사용하는 것이 공인인증서와 공인인증서 비밀번호(개인키에 접근할 수 있는 비밀번호)이다. 공인인증서는 일반적으로 컴퓨터의 하드디스크 혹은 이동식디스크 등에 파일형태로 저장된다. 또한 실제 전자서명 생성을 위해 사용되는 개인키는 본인만 사용해야 하므로 암호화하여 공인인증서 파일과 같은 위치에 파일 형태로 저장한다. 이처럼 파일로 저장되므로 파일 복사를 통해 동일한 공인인증서를 생성할 수 있다[15].

이러한 특성 때문에 해킹 등 내·외부의 공격으로 공인인증서가 복사되는 상황이 발생될 수 있다. 최근에는 개인컴퓨터 해킹 뿐 아니라 스마트폰을 이용한 전자금융서비스가 증가하면서 스마트폰에 공인인증서를 저장하여 이용하는 일이 많아졌다. 하지만 악성코드에 감염되어 스마트폰에 저장된 공인인증서가 유출(해커들의 공인인증서 탈취)되는 사례가 발생되고 있다. 공인인증서를 탈취한 해커들은 공인인증서 비밀번호가 필요함에 따라 비밀번호를 유추하거나 보이스 피싱 등을 통해 비밀번호를 취득하여 이를 비대면 전자거래에서 본인 인증수단으로 활용한다.

이에 따라 공인인증서의 안전성을 강화하기 위한 다양한 정책 및 제도들이 시행되었다. 공인인증서에 대한 위험도는 미국 연방정부, 일본 법무성 등 다양한 국가에서 사용하는 국제표준인 PKI(공개키 기반구조)를 기반으로 한 인증기술이므로 낮다고 보고 공인인증서 저장 및 비밀번호 보관 및 사용 등에 관한 정책 및 제도에 집중된다. 2011년부터 공인인증서를 발급 및 저장할 때 하드디스크를 이용하는 경우에는 해킹 등에 취약하다는 내용을 알려주는 경고화면을 띄우고 있으며 2013년부터 인증서를 발급 받거나 300만 원 이상 이체를 할 경우에는 단말기 지정 또는 ARS인증 등의 추가 인증을 하거나 OTP(One Time Password)를 사용하도록 하였다[16]. 또한 2014년 9월부터 공인인증서 비밀번호 설정 규칙을 숫자, 영문, 특수문자 중 2종 이상으로 조합된 8자리이상 사용에서 숫자, 영문, 특수문자를 반드시 포함한 10자리 이상으로 강화하였다. 또한 공인인증서를 저장할 때는 공용메모리에 저장이 아닌 USIM이나 보안토큰(키 생성 또는 전자서명 생성 등이 기기 내부에서 처리 되도록 PKCS#11(암호토큰 인터페이스 표준)에 따라 구현한 기기)과 같은 안전한 저장매체에만 저장하도록 권고하고 있다[17,18]. 하지만 보안토큰을 지원하지 않는 웹사이트에서는 사용이 불가능하고 USIM에 저장한 경우에는 이동통신사를 변경하면 USIM도 변경해야하는 불편함이 존재한다. 이에 따라 공인인증기관에서는 하드웨어 형태가 아닌 소프트웨어 형태의 보안토큰을 구현(공인인증서 파일 유출을 방지할 수 있도록 키 접근제어 및 하드웨어 정보기반 암호화 기술 등을 적용한 인증서 저장방식)하여 제공하고 있다.

3.2 공인인증서 갱신 관리

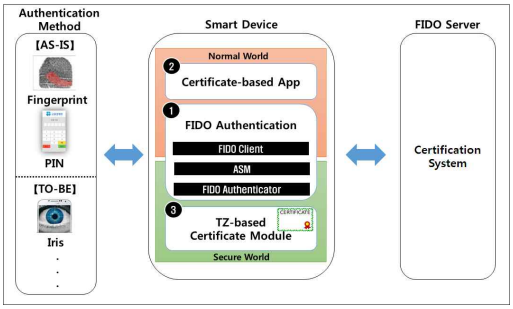
보다 안전한 공인인증서 사용을 위해 공인인증서 유효기간을 1년으로 정함에 따라 매년 공인인증서를 갱신 또는 발급해야 하는 번거로움이 발생하고 있고 공인인증서를 저장한 매체를 소지하고 다녀야 하는 불편함이 발생하고 있다. 따라서 공인인증서를 다수 복사하여 사용하는 매체에 저장하는 사람도 생겨남에 따라 공인인증서 유출에 노출되고 있다. 또한 타 기관에 이용하기 위해서는 복잡한 절차를 거쳐 등록해야 하는 어려움이 사용자의 불편을 초래하고 있다.

3.3 공인인증서를 이용키 위한 환경

웹브라우저가 제공하는 기능으로는 공인인증서 발급이나 전자서명 등을 처리할 수 없기 때문에 공인인증기관으로부터 공인인증서를 발급받거나 전자서명을 생성하기 위해서는 공인인증 가입자 소프트웨어라고 불리는 별도의 프로그램이 필요하다. 또한 개인방화벽이나 키보드보안 프로그램을 별도로 설치하라며 다운로드를 요구하는 것도 웹브라우저에는 기능이 없기 때문에 보안성을 위해 취해지는 조치이다. 최근 언론매체를 통해 액티브X가 전자상거래 이용에 불편을 준다는 보도로 공인인증서를 사용하지 말자고 주장하는데 이는 액티브X를 이해하지 못한데서 오는 것으로 보인다. 액티브X는 마이크로소프트사의 웹브라우저인 익스플로러를 사용할 때 익스플로러가 기능을 지원하지 않아 필요한 기능을 이용할 수 있도록 지원하는 인터페이스이다. 이에 대한 이해부족으로 공인인증서 사용이 불편하니까 공인인증서 폐지까지 거론되고 있는 실정이다.

4. FIDO 기반의 생체기술과 안전영역을 연계한 공인인증서의 효율성 강화 방안

3장에서 살펴 본 바와 같이 공인인증서를 하드디스크 등에 파일형태로 저장함에 따른 유출을 방지하는 공인인증서의 안정성 강화와 별도 소지에 따른 불편함을 개선하는 등의 편리성을 강화할 필요가 있는 바, 본고에서는 FIDO 생체기술과 안전영역을 연계한 공인인증서 효율화 방법을 [Fig. 8]와 같이 제안하고자 한다.



[Fig. 8] Service Architecture

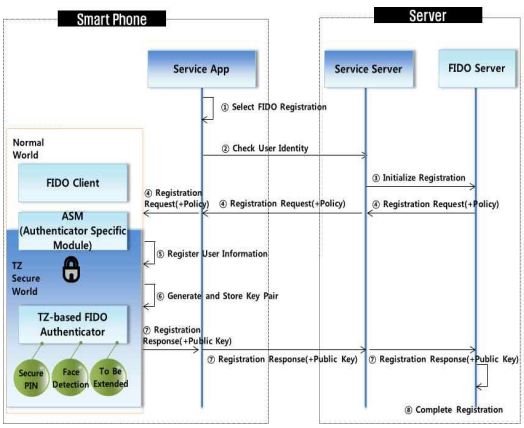
위 그림에서 보는 바와 같이 고객이 소지하고 있는 스마트폰의 안전영역에 공인인증서를 저장하고 공인인증서를 이용하려는 사용자 인증을 FIDO 생체인식 기술을 기반으로 수행[19,20]하는 방법을 말한다. 즉 공인인증서와 개인키를 보안토큰 기능이 있는 안전영역 내에 안전하게 저장함으로써 기존 일반 디스크 등에 파일 형태로 저장되어 발생되는 유출을 방지하는 등의 안전성을 확보하는 동시에 공인인증서 비밀번호를 대신하여 간편한 FIDO 생체기술 인증만으로 공인인증서를 이용할 수 있게 됨으로서 편리성을 확보하게 된다[21].

세부적으로 살펴보면 <Table 3>과 같이 안전영역(TrustZone)기반 공인인증모듈은 공인인증서 발급 및 저장과 전자서명 기능을 제공하며 FIDO 인증모듈과 연계하여 공인인증서 비밀번호 입력대신 생체인식으로 대체한다. FIDO 인증모듈은 공개키와 개인키를 생성하여 개인키는 스마트폰 안전영역인 저장소에 저장하고 공개키는 FIDO 서버에 보관하여 전자서명 및 검증을 수행한다.

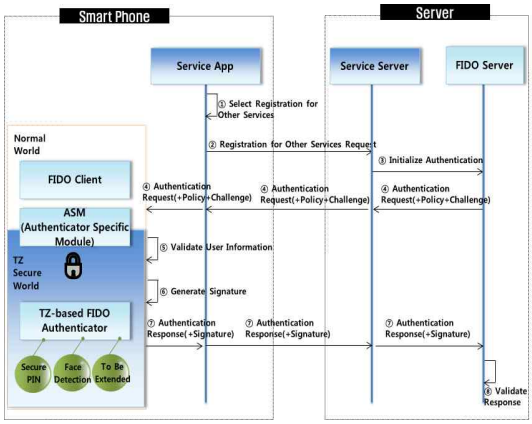
<Table 3> Main Functionalities

FIDO Authentication	TZ-based FIDO Authenticator	TZ-based FIDO Registration and Authentication
	ASM, FIDO Client	Integration of FIDO Authenticator with Certificate-based Apps
TZ-based Certificate Module		TZ-based Certificate Mgt./ Integration of Certificate Password and FIDO Biometrics
Certificate-based App		Service using FIDO Authentication Module
FIDO Server		FIDO Registration and Authentication

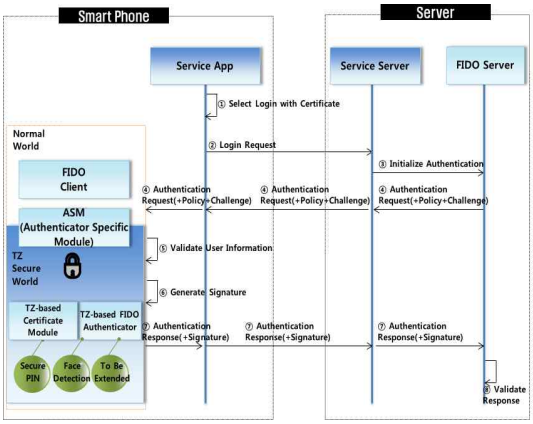
FIDO 생체기술과 안전영역을 이용한 효율화 강화 방법에서 필요한 세부 업무처리 절차들은 ① 고객이 신규로 FIDO 모듈을 설치하고 FIDO 서비스를 등록하는 [Fig. 9] FIDO 등록 업무절차, ② 기 등록한 FIDO 서비스를 별도의 사용자 정보 등록이나 공개키 등록 없이 [Fig. 10] 타 기관등록(해지)하는 업무절차, ③ 앱에서 FIDO 서비스를 이용하는 로그인하는 [Fig. 11] FIDO 이용 로그인 업무절차, ④ 앱에서 FIDO 서비스를 이용하여 이체를 하는 [Fig. 12] FIDO 이용 이체 업무절차, ⑤ 앱에서 안전영역기반 공인인증모듈을 이용하여 로그인하는 [Fig. 13] FIDO 기반의 공인인증서 이용 로그인 업무절차, ⑥ 앱에서 안전영역기반 공인인증모듈을 이용하여 이체하는 [Fig. 14] FIDO 기반의 공인인증서 이용 이체 업무절차가 있다.



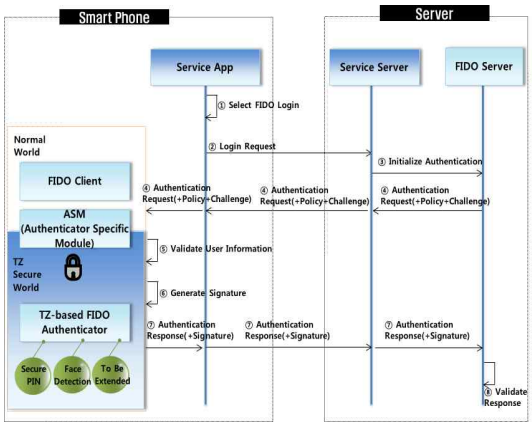
[Fig. 9] FIDO Registration



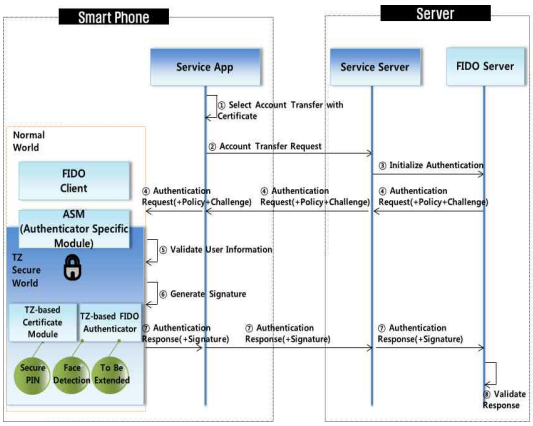
[Fig. 10] Registration(Deregistration) for Other Services



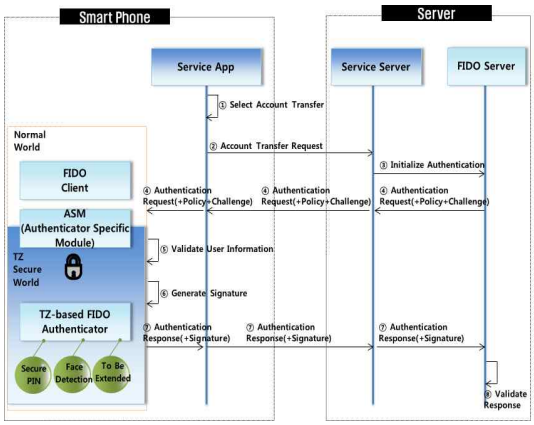
[Fig. 13] Login with Certificate(FIDO)



[Fig. 11] Login Using FIDO



[Fig. 14] Account Transfer with Certificate(FIDO)



[Fig. 12] Account Transfer Using FIDO

5. 요약 및 결론

전자서명법에 따라 발급되고 있는 공인인증서는 비대면 거래에서의 필수 기능인 인증, 인가, 기밀성, 무결성, 부인봉쇄 기능을 제공하기 때문에 전자금융거래, 전자민원 등 다양한 분야에 이용되고 있다. 하지만 공인인증서는 파일로 저장할 경우 해커로 인한 유출이 가능하며 이용 시 별도 프로그램 설치가 필요하기 때문에 안전성, 편리성 양 측면에서 비판을 받고 있는 것도 사실이다. 특히 최근에는 안전성 뿐 아니라 편리성이 강조된 인증수단에 대한 요구가 늘어나 인증 관련기관은 물론 정부에서도 다양한 인증수단 개발을 시도하고 있다.

이에 따라 본 고에서는 현재 3000만 장 이상 사용되고

있는 공인인증서의 안전성과 편리성을 강화하기 위해 FIDO 생체기술과 안전영역을 결합한 새로운 형태의 인증수단을 제시하였다. 특히 제시된 모델은 별도의 장치 없이도 현재 대부분의 최신 스마트폰에 기본 탑재된 생체정보 인식기능와 ARM 프로세서의 안전영역을 이용하였다는 점에서 서비스의 적용이 용이하다는 장점이 있다.

향후 연구에서는 제시된 방식을 이용하여 생체정보와 공인인증서를 실제로 연계하고 다양한 생체정보 별로 안전성과 편리성을 분석해보고자 한다. 또한 모바일 환경뿐 아니라 PC 환경에서의 공인인증서의 안전성과 편리성을 개선하는 방법도 연구가 필요하다. 본 고에서 제시된 방법이 실 서비스에 적용되어 비대면 전자거래에서의 공인인증서 이용환경이 더 안전하고 편리해지길 기대해 본다.

REFERENCES

[1] RSA Laboratories, “PKCS #1 v2.2: RSA Cryptography Standard”, 2012.

[2] National Law Information Center, “Digital Signature Act”, http://www.law.go.kr (June, 2017)

[3] Kyung-Hye Park, "A study of the scenario for improvement of NPKI system", Journal of Digital Convergence, Vol. 8, No. 4, pp. 59-71, 2010.

[4] Korea Internet & Security Agency, “Digital Signature Certificate Profile”, 2009.

[5] Korea Internet & Security Agency, “Accredited Digital Signature Certificate Revocation List Profile”, 2009.

[6] Han-Wook Lee, “Current Status and Future Prospects of FIDO Authentication Technology”, KFTC Payments Trends, Vol. 261, 2016.

[7] Jae Jung Kim and Seung Phil Hong, “Design of a Secure Biometric Authentication Framework Using PKI and FIDO in Fintech Environments”, International Journal of Security and Its Applications, Vol. 10, No. 12, pp. 69-80, 2016.

[8] Hyun-Joong Kim, Byung-Rae Cha and Sung-Bum Pan, "Technology Trends, Research and Design of AIM Framework for Authentication Information Management", Journal of Digital Convergence, Vol. 14, No. 7, pp. 373-383, 2016.

[9] FIDO Alliance, http://fidoalliance.org (June, 2017)

[10] Young-Joon, Choi, “Digital Certificates Usage and Technology Trends in Smartphone”, KFTC Payment Systems and Information Technology, Vol. 56, 2014.

[11] GlobalPlatform, "Trusted Execution Environment(TEE) Guide", https://globalplatform.org/mediaguidetee.asp (June, 2017)

[12] ARM Ltd., https://www.arm.com/products/security-on-arm/trustzone (June, 2017)

[13] Jeong Nyeo Kim, "Security Core Technology Implementation for Hardware-based Smart Devices", Journal of Digital Convergence, Vol. 14, No. 11, pp. 501-505, 2016.

[14] Hwi-Min Choi, Chang-Bok Jang and Joo-Man Kim, “Efficient Security Method Using Mobile Virtualization Technology And Trustzone of ARM”, Journal of Digital Convergence, Vol. 12, No. 10, pp. 299-308, 2014.

[15] Keyong-Seog Song, "A Study on the Risk Management of e-Finance by Active Internet", Journal of Digital Convergence, Vol. 8, No. 2, pp. 189-202, 2010.

[16] Financial Services Commision, “Electronic Financial Fraud Prevention Service Press Release”, 2013.

[17] Korea Internet & Security Agency, “User Interface Specification for the Interoperability between Accredited Certificate Authorities”, 2015.

[18] Korea Internet & Security Agency, “Certificate Management in Mobile Device”, 2015.

[19] Hyeon-Joon Moon, Min-Hyung Lee and Kang-Hun Jeong, "Authentication Performance Optimization for Smart-phone based Multimodal Biometrics", Journal of Digital Convergence, Vol. 13, No. 6, pp. 151-156, 2015.

[20] Sunghyun Yun, "The Biometric Signature Delegation Method with Undeniable Property", Journal of Digital Convergence, Vol. 12, No. 1, pp. 389-395, 2014.

[21] Korea Internet & Security Agency, “Implementation Guideline for Safe Usage of Accredited Certificate using bio information in Smart phone”, 2016.

조 화 건(Cho, Hwa Gun)

- 1985년 2월 : 충북대학교 컴퓨터공학과 졸업(학사)
- 2006년 2월 : 고려대학교 경영대학원 경영과학및MIS전공 졸업(석사)
- 2011년 1월 ~ 2013년 7월 : 금융결제원 e사업전산실장
- 2013년 7월 ~ 2015년 1월 : 금융결제원 IT기획부장
- 2015년 1월 ~ 2015년 4월 : 금융결제원 전자금융부장
- 2015년 4월 ~ 현재 : 금융결제원 정보보호본부장
- 관심분야 : 전자인증, 전자금융, 정보보호
- E-Mail : hwagun@kftc.or.kr

양 해 술(Yang, Hae Sool)

- 1975년 2월 : 홍익대학교 전기공학과 졸업(학사)
- 1978년 8월 : 성균관대학교 정보처리학과 졸업(석사)
- 1991년 3월 : 日本 오사카대학 정보공학과 SW공학 전공(공학박사)
- 2006년 2월 : Kazakhstan 유러시안 경제대학(명예경영학박사)
- 1975년 5월 ~ 1979년 6월 : 중경단 전산실 시스템 분석장교
- 1980년 3월 ~ 1995년 5월 : 강원대 전자계산학과 교수
- 1986년 12월 ~ 1987년 12월 : 日本오사카대학 객원연구원
- 1995년 6월 ~ 2002년 12월 : 한국 Software 품질연구소장
- 2010년 3월 ~ 2012년 2월 : 호서대학교 창업대학원 원장
- 2012년 11월 : 대통령표창(SW산업발전유공) 수상
- 1999년 11월 ~ 현재 : 호서대학교 벤처대학원 교수
- 관심분야 : SW공학(특히, SW품질보증과 품질평가, 품질관리 및 컨설팅, SI), SW프로젝트관리, 품질경영
- E-Mail : hsyang@hoseo.edu