Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1049

FIDO2 CTAP을 활용한 전자서명 방법*

조 한 구,† 이 경 호‡
고려대학교 정보보호대학원

A Method of Digital Signature Using FIDO2 CTAP*

Han-koo Cho,† Kyung-ho Lee‡
Korea University Graduate School of Information Security

요 약

국가 공인인증서는 미리 신원 확인된 사용자 개인정보에 기초하여 발급된 사용자인증서로서 대부분의 전자금융거래와 사용자 인증에 활용되는 보편적인 인증수단이 되었으며 전자정부와 국내 이용편익에 많은 기여를 하였다. 그러나 이용방법에 대한 웹 표준규격의 부재로 인하여 별도의 플러그인을 설치하는 등의 불편함이 따랐고 이를 개선하고자 하는 노력이 지속되어 왔다. 본 논문에서는 FIDO2 (Fast Identity Online v2) CTAP(Client to Authentication Protocol) 규격 내 확장(extension) 영역을 활용한 인증서 전자서명 방법을 제시함으로써 인증서 이용환경에 대한 문제점을 해결하고자 한다.

ABSTRACT

The national accredited certificate is a user certificate issued based on the user's personal information, which has been identified in advance, and has become a universal authentication method used for most electronic financial transactions and user authentication. And it contributed a lot to the use of e-government and domestic service. However, due to the lack of web standards on how to use, it was inconvenient to install a separate plug-in, and efforts to improve it have been continued. In this paper, we attempt to solve the problem of certificate usage environment by presenting the certificate digital signature method using the extension of the FIDO2 (Fast Identity Online v2) client to authentication protocol (CTAP) specification.

Keywords: FIDO2, CTAP, WebAuthn, Certificate, ActiveX, Plug-in

I. 서 론

국내에서 과거 20 여 년간 이용되어 왔던 공인인증서는 전자서명법에 명시된 인증서의 효력 및 부인방지 기능, 그리고 한 번 발급되면 모든 이용 사이트에 동일하게 적용될 수 있는 상호연동성을 바탕으로 개인과 기업 전반에 배포되었다. 인터넷뱅킹, 온라인 주식거래, 온라인 쇼핑 등 거래의 부인방지가 요구되는 대부분의 전자금융거래에서 전자서명을 생성할 수 있는 공인인증서의 활용은 집중 되어졌다. 국가정보화백서에 의하면 2017년 인터넷뱅킹 이용 건수 9,647만 건(3/4분기 기준), 스마트폰뱅킹 이용 건수 5,985만 건(4조 1379억원)이며 모바일뱅킹 등록 고객 수 8,766만 명, 온라인쇼핑 거래액 6조 3,333억으로 집계되고 있다[26]. 전자금융거래 외에도 범

Received(08. 06. 2019), Modified(09. 30. 2019), Accepted(10. 02. 2019)
* This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2019-2015-0-00403) supervised by the IITP (Institute for Information & communications Technology Planning & Evaluation)
† 주저자, forum19@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

용 공인인증서가 있으면 전자정부 민원서비스, 4대 사회보험, 국세청 홈텍스, 전자세금계산서, 전자입찰/조달, 온라인교육, 예비군 등 다양한 분야의 업무를 하나의 공인인증서만으로 인터넷을 통해 편리하게 이용할 수 있게 되었다[27]. 하지만 인터넷 환경이 고도화됨에 따라 비표준 이용방식의 문제점도 보이고 있다. 사이트별로 각종 플러그인 설치를 해야 하고 피싱이나 저장소 해킹 등 보안사고도 끊이지 않고 있다[3]. 또한 공인인증서 이용 강제성으로 다양한 인증수단의 확산을 막는다는 의견이 있었다. 이러한 불편함과 보안 취약성을 개선시키고자 여러 기술적 시도가 있었지만 여전히 특정 한계를 극복하기 어려웠다. EXE 프로그램 설치방식은 플러그인 설치는 아니지만 사용자 PC 에 서비스 에이전트를 설치해야 하는 불편함이 남아있다. Html5 스크립트에 기반한 인증서 이용방식은 브라우저에 종속된 저장기술로서 브라우저 프로그램이나 플러그인 설치 없이 이용 가능하지만 캐시메모리를 초기화 하는 경우 인증서를 재설치 해야 한다. 전자금융거래에서 공인인증서 의무사용 폐지에 따라(2015.3.18.) 사설인증서나 핀(PIN) 기반의 인증방식도 등장했다. 두 방식 모두 패스워드 입력이 없어 편리할 수 있으나 해당 사이트에서만 적용되는 인증방식으로 사용자는 사이트별로 개인 신원확인 절차를 거쳐야 한다.

FIDO(Fast Identity Online) 는 국내외 산업 전반에 도입이 확산되고 있는 생체인증과 관련한 비암호인증(passwordless authentication) 규격이다. 최근 발표된 FIDO2 버전은 CTAP(Client to Authenticator Protocol) 규격이 ITU-T 표준으로 등재되었으며[1][2] WebAuthn API 가 W3C 웹 표준으로 등재되었다[15]. 따라서 사용자는 PC 와 모바일의 웹환경에서 별도의 프로그램 설치 없이 FIDO 인증 서비스를 이용할 수 있게 되었다. FIDO 기술규격이 반영된 생체인증이 공인인증서를 대체할 수 있을지 여부는 보다 연구가 필요한 부분이다. FIDO 등록 및 인증단계에서 인증서를 사용하고 전자서명을 수행하지만 FIDO 인증장치 내의 증명용 인증서(Attestation Certificate) 는 사용자인증서가 아닌 기기인증서이므로 사용자 신원확인이 전제되지 않는다. 따라서 FIDO 규격 자체만으로 공인인증서처럼 부인방지 효과를 지니는가에 대하여는 논쟁의 소지가 있다[4].

본 논문에서는 FIDO 프로토콜 상에 공인인증서의 저장과 이용을 추가 반영하는 모델을 제안한다. 또한 이 모델이 성공적으로 동작하는지 실험방법을 제시하고 결과를 기술하였다. 결론적으로 PC 클라이언트에서 CTAP을 이용한 인증을 진행할 때 FIDO 웹표준 API 만을 사용하므로 패스워드 입력이 없을 뿐만 아니라 별도의 프로그램이나 플러그인 설치 없이 기존 공인인증서의 사용이 가능하게 되었다.

II. 선행연구

PKI 기술이 고도화된 국내 환경에서는 FIDO1.0 이 보급되는 시점부터 FIDO 기술과 전자서명 기술을 접목하여 인증서 이용환경을 개선하려는 연구들이 진행 되었다.

2.1 PKI 와 전자서명

PKI(Publick Key Infrastructure) 는 공개키 암호기술(Public Key Cryptography)을 구현한 양자간 통신에서 사용된 공개키 또는 개인키의 소유증명이나 키의 유효성을 검증할 수 있도록 구성된 기반구조이다[19]. PKI 는 이미 표준화된 응용기술인 SSL/TLS, S/MIME 등이 전 세계적으로 널리 쓰이고 있으며 특히 사용자 거래의 무결성 및 부인방지가 필요한 전자계약, 전자금융거래에 전자서명 기술이 사용되고 있다. PKI 와 전자서명 기술은 암호학적 우수성을 지닐 뿐 아니라 신뢰기관(Trusted Anchor)을 기반으로 한 인증키의 라이프사이클이 보장되면 강력한 상호연동성을 제공할 수 있다. 이러한 특성들은 국내 공인인증제도와 전자서명법 도입, 공인인증서의 발급과 인터넷뱅킹, 온라인주식거래, 전자민원 등의 대국민 서비스 구축을 촉진 시켰다 할 수 있다[7][16]. 최근 들어 표준화된 FIDO 규격 또한 PKI 기반기술이 반영된 것으로 사용자 인증과 거래의 보안성과 편의성을 높여 줄 것으로 예상된다[20]. 국외에서는 아시아(대만, 일본, 싱가포르, 중국) 와 북미(미국, 캐나다), 유럽(벨기에, 독일, 에스토니아, 핀란드) 등의 국가에서 정부 또는 민영기관이 PKI 시스템을 구축하여 다양한 서비스를 제공하고 있다[18].

2.2 공인인증서

우리나라의 전자서명 공인인증제도는 1999년 2월 5일 전자서명법 (법률 제5792호)이 제정과 함께,

1999년 7월 1 일자로 시행되었다[10]. 2000년에는 전자입찰, 2001년부터 2005년에는 인터넷 뱅킹, 온라인 증권, 2006년부터 2009년에는 주택청약, 연말정산, 2010년에는 스마트폰 뱅킹, 2011년에는 전자세금계산서 분야까지 공인인증서의 이용이 도입되었다. 인터넷사용자 중 64.5%가 최근 1년 이내 인터넷을 통해 상품이나 서비스를 구매한 것으로 나타났다. 2011년 7월 인터넷 사용자수를 기준으로 환산하면 약 2,400만 명이다. 인터넷 뱅킹의 경우 이용률은 42.4%로서 마찬가지로 환산하면 약 1,567만 명이다. 인터넷 주식거래의 경우 만 18세 이상 사용자의 9.9%가 최근 1년 이내에 인터넷을 통해 주식거래를 한 것으로 나타났다. 이처럼 공인인증서의 이용분야는 증가하였고, 공인인증서 발급 수 역시 증가하였다. 한국은행 보도자료에 의하면 2015년 3월말 현재 인터넷뱅킹서비스 등록 고객수는 1억 861만 명으로 증가하였고 인터넷뱅킹 공인인증서 발급건수는 2841만 건으로 나타났다[7]. 공인인증서는 20여년간 사용자 인증 및 전자서명의 보편적 수단으로 자리잡았을 뿐만 아니라 지속적인 기능 개선과 보안강화 연구가 이루어져 왔다[16]. 그러나 공인인증서는 윈도우 운영체제의 인터넷 익스플로러 환경에서 사용되는 액티브X에 기반하고 있어 다른 웹브라우저에서는 사용하기 어려운 문제가 있다. 또한 공인인증서는 사용자 PC나 USB에 파일로 저장될 수 있기 때문에 안전성 문제도 제기되고 있다[11].

2.3 FIDO 1.0 인증기술

FIDO 1.0 인증 기술은 현재 사용자가 인증서 등과 같은 인증 수단을 소지하고, 패스워드 입력에 따른 보안 문제점을 극복하고자 개발되었다. FIDO 1.0 인증 기술은 UAF(Universal Authenticator Protocol) 방식과 U2F(Universal 2nd Factor) 방식을 제공한다. UAF 인증 방식은 기존의 ID/Password 인증 방식보다 보안이 강화된 개인의 생체 정보를 활용하는 표준이며, U2F는 ID/Password 인증 방식에 별도의 인증 장치를 추가적으로 사용하는 방식이다[12][13].

FIDO UAF 규격은 스마트폰을 중심으로 설계되었으므로 PC, IOT 기기에 적용이 어렵고, UAF와 U2F 모두 사용자인증서를 고려하지 않은 규격이므로[14][17] 국내 공인인증서와 성격이 다른 인증규격으로 간주되었다.

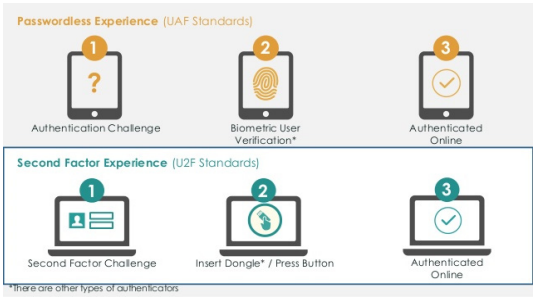

Fig. 1. FIDO 1.0 UAF / U2F[37]

2.4 K-FIDO

국내에서는 2016년부터 스마트폰의 지문센서 및 안전한 저장공간을 이용하여 공인인증서의 패스워드 입력을 제거한 K-FIDO[5] 와 복수기기에서 K-FIDO를 효율적으로 활용하는 방안이 제기 되었다[6]. 사용자는 패스워드를 기억하지 않아도 지문 등의 생체인증을 통하여 공인인증서 전자서명이 가능하게 되었다. 하지만 이 규격은 FIDO1.0 UAF 규격을 공인인증서 이용환경에 접목한 것으로서 스마트폰 또는 스마트카드에 사용성이 제한되어 있다. PC와 웹환경에 적용하려면 인증서 전자서명에 기반한 서명응답을 웹브라우저에서 처리하기 위한 플러그인이 별도로 필요하다는 문제가 여전히 해결되지 않는다.

2.5 FIDO2 와 공인인증서

FIDO2 WebAuthn API 가 인터넷 표준으로 지정됨에 따라[15] 패스워드를 대체할 수 있는 사용자 인증(생체인증, PIN 인증)이 웹브라우저 상에서 플러그인 설치 없이 서비스가 가능하게 되었다. 그러나 FIDO2 는 상호연동성을 제공하지 않으므로 사용자는 서비스 별로 별도의 가입절차를 따라야 하는 번거로움이 발생한다. 반면, 국내 공인인증서는 상호연동성을 바탕으로 한 번 발급받으면 대부분의 사이트에서 쉽게 인증을 받을 수 있으나 이용환경에 대한 표준의 부재로 인하여 편의성이 낮고 보안이 취약하다. 따라서 FIDO2 와 공인인증서는 서로의 특성이 상보적 관계를 지닌다 할 수 있으며 서로의 장점을 보완하여 이용할 수 있다면 사용자 인증의 중요한 개선을 기대할 수 있다. 이러한 시도는 2018년에 한국전자통신연구원의 특허로 등록된 바 있다.

대한민국 공개특허 제10-2018-0028751호(2018.03.19.)에 기재된 "FIDO 2.0에서 인증서를 이용한 사용자 인증 방법 및 장치"는 FIDO 기반 디바이스를 인증서 기반 사용자 인증에 사용하는 방식을 제안한다[9]. 이 방식에 따르면, 인증장치는 등록 요구를 수신하면 생체정보 등으로 사용자를 확인하고 인증서 기반의 인증키를 생성하여 assertion 메시지에 포함시켜 응답하여 등록하게 할 수 있고, 로그인, 쇼핑, 금융 등 서비스를 이용하고자 하는 네트워크 상의 다른 서버로부터의 인증 요청에 따라 인증키를 해당 서버로 전송하여 인증을 받도록 할 수도 있다. 그러나 이 방식에서는, 인증장치의 (디바이스) 전자서명값 대신 사용자인증서 전자서명을 사용하기 때문에 FIDO 보안목표(security goal)를 벗어나는 구조이다[8].

III. 모델 제시

3.1 배경

본 고에서 제안하는 모델의 목적은 공인인증서와 같은 사용자인증서 전자서명의 불편한 이용환경을 개선하고자 함이다. 선행연구를 통하여 최근 국제표준 등재가 완료된 FIDO2 CTAP 규격이 인증서의 이용환경을 개선하는데 가장 적합한 것으로 판단되었으며 그 이유는 다음과 같다.

1. 인증서의 등록절차는 FIDO2 규격의 등록절차와 기본적으로 동등한 구조를 갖는다.
2. 인증서 전자서명 과정은 FIDO2 규격의 인증과정과 기본적으로 동등한 구조를 갖는다.
3. FIDO2 CTAP 규격의 확장영역은 서비스주체가 정의하고 이용할 수 있다.

위와 같은 성질을 이용하여 웹브라우저에 기반한 서비스 환경에서 사용자인증서 및 개인키를 인증장치에 저장하는 과정과 인증장치 내 사용자개인키로 전자서명을 생성하여 제출하는 과정을 FIDO2 규격 내에서 실시하는 모델을 제시한다. 본 모델에 의하여 사용자는 플러그인과 같은 부가적인 프로그램을 설치할 필요가 없을 뿐 아니라 인증서 패스워드를 지문 등의 생체인식으로 대체함으로써 패스워드 도용, 유출의 문제를 해결할 수 있게 되었다.

3.2 FIDO2 서비스시스템 구성

FIDO2 가 동작하는 정상적인 시스템 구조는 fig 2와 같다. 클라이언트 단에서는 운영체제 역할을 하는 플랫폼과 웹표준 API 가 동작 가능한 브라우저와 그 위에서 동작하는 웹서비스 프로그램(Relying Party Application) 및 FIDO2 인증장치(Authenticator)로 구성된다.

FIDO2 인증장치는 내부 인증장치(Internal Authenticator) 와 외부 인증장치(External Authenticator) 로 나뉜다. 외부 인증장치는 동글장치, 스마트폰, 스마트카드, 웨어러블 기기등 될 수 있으며 PC 의 클라이언트 플랫폼(CP)과 USB, BLE, NFC 의 방법으로 통신을 한다. CTAP 규격은 인증장치와 CP(Client Platform) 의 표준화된 통신 규격이다. 서버 단에서는 서비스를 제공하는 RP 서버 및 FIDO2 인증을 담당하는 FIDO 서버로 구성된다. FIDO2 서비스는 등록과 인증의 과정으로 구분된다. FIDO2 등록은 FIDO2 서비스를 이용하는 사용자의 인증키를 등록하는 과정이다. 이 때 인증장치에서는 makeCredential 메시지가 생성되고 플랫폼과 브라우저를 거쳐 FIDO2 서버로 전송된다. FIDO2 인증은 인증장치 내 저장된 인증키로 전자서명값을 제출하는 과정이다. 이 때 인증장치는 getAssertion 메시지가 생성되고 등록과 같은 방식으로 서버에 전달된다.

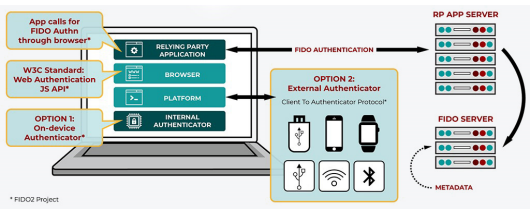

Fig. 2. FIDO2 System Architecture[37]

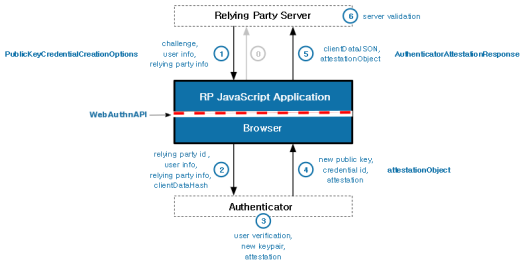

Fig. 3. FIDO2 Registration Flow[37]

3.3 모델의 개요

FIDO2는 등록(registration)과 인증(authentication) 단계로 구분된다. 일반적인 사용자인증서 서비스 또한 인증서 등록과 전자서명 단계로 구분되므로 FIDO2 서비스와 사용자인증서 서비스의 단계는 서로 매칭될 수 있다. 사용자인증서를 서버에 등록하는 과정은 FIDO2에서 정의된 등록 단계에서 인증장치 내 저장된 사용자인증서를 makeCredential 메시지에 포함시켜 서버로 전송하는 방법이다. 개인키 전자서명 과정은 FIDO2 에서 정의된 인증단계에서 getAssertion 메시지에 인증장치 내에서 사용자개인키로 서명한 값을 포함시켜 서버에 전송하는 과정이다. 인증장치에서 생성된 각 메시지는 FIDO2 CTAP 규격에 의하여 웹브라우저로 전송되고 웹브라우저에서는 FIDO2 규격에 관한 오류 체크 및 수신한 메시지를 JSON 타입으로 인코딩 후 서버로 전송한다.

3.4 makeCredential과 사용자인증서 등록

FIDO2 등록단계에서는 인증장치에서 생성된 makeCredential 메시지가 CTAP 프로토콜에 의해 웹브라우저를 거쳐 서버로 전송된다. 이 때 인증장치 내 저장된 사용자인증서 정보를 authData extension 위치에 삽입하여 makeCredential 메시지를 인코딩 하도록 인증장치 프로그램을 구현한다. FIDO2 서버는 수신한 makeCredential 메시지 내 사용자인증서 정보를 추출하여 DB 에 저장한다.

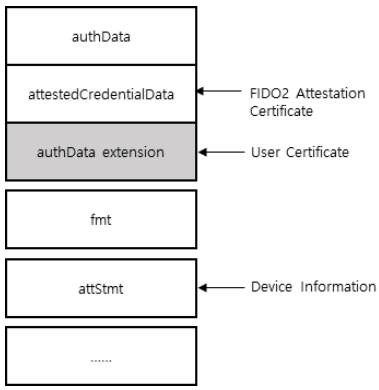

Fig. 4. FIDO2 makeCredential message

3.5 getAssertion 과 전자서명

FIDO2 인증단계에서는 인증장치에서 생성된 getAssertion 메시지가 CTAP 프로토콜에 의해 웹브라우저를 거쳐 서버로 전송된다. 이 때 인증장치 내 사용자개인키에 의해 전자서명된 정보를 authData extension 위치에 삽입하여 getAssertion 메시지를 인코딩 하도록 인증장치 프로그램을 구현한다. FIDO2 서버는 수신한 getAssertion 메시지 내 전자서명 정보를 추출하여 전자서명을 검증한다.

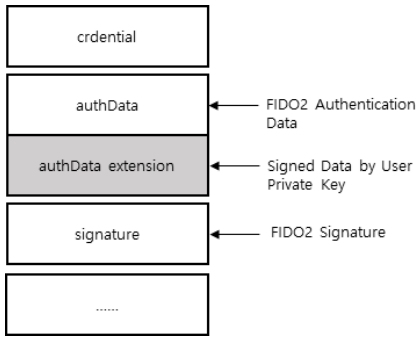

Fig. 5. FIDO2 getAssertion message

3.6 동작 흐름도

본 절에서는 FIDO2 등록과 인증의 기본적인 동작흐름을 기술하고 동일한 흐름도에 사용자인증서 등록과 전자서명 제출과정을 접목시키는 방법을 제시한다.

3.6.1 FIDO2 등록(registration)

FIDO2 등록은 사용자가 최초로 서비스를 이용하고자 할 때 인증장치를 통하여 생체인증(user verification)을 한 후 서버가 요청한 값에 대한 결과값을 인증장치를 통하여 서버에 제출 및 검증하는 과정이다. 일반적인 FIDO2 인증절차는 다음과 같다.

step1. CP(Client Platform , 웹브라우저)는 서버에 접속 후 서버로부터 makeCredential 요청메시지(publicKeyCredentialCreationOptions)를 수신한다. (이 메시지는 서비스 서버의 URL 같은 서버 정보와 사전 본인확인을 거친 사용자의 정보가

선택적으로 들어갈 수 있다.)
step2. CP는 수신한 요청메시지를 인코딩한 후 (authenticatorMakeCredential) 주단말기와 연결된 인증장치에게 전달한다. 이 과정에서 CP는 clientDataHash 를 추가시키는데 이는 이 값이 인증장치 서명원문의 일부가 되게 함으로써 보안성을 높이기 위함이다.
step3. 요청메시지를 수신한 인증장치는 해당서비스를 위한 인증용 키쌍을 생성하고 인증용공개키(authentication public key)를 안전하게 전달하기 위한 attestation 을 생성한다. 이 과정에서 인증장치는 생체인증 등 로컬 단에서 사용자를 인증하는 과정(user verification)을 선택적으로 포함시킬 수 있다.
step4. 인증장치는 attestation 메시지를 정의된 타입(CBOR)[29]으로 인코딩한 후 CP로 전송한다. (attestationObject)
step5. 응답메시지를 수신한 브라우저는 적절한 타입으로 메시지를 인코딩 후 서버로 전송한다. (authenticatorAttestationResponse)
step6. CP로부터 응답메시지를 수신한 서버는 해당 attestation 메시지 및 인증장치의 증명용인증서(attestation certificate)의 유효성을 해당 인증장치의 발급자 인증서를 포함한 메타데이터(metadata)를 이용하여 검증한다. 검증이 성공하면 공개키를 DB 에 저장한다.

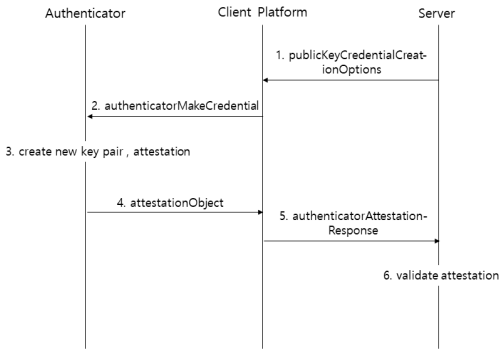

Fig. 6. Basic FIDO2/WebAuthn user flows : FIDO2 Registration

3.6.2 사용자인증서 등록

사용자인증서의 등록과정은 앞 절 FIDO2 등록과정에 포함된다. step1과 step2는 앞 절과 동일하다. step3에서 인증장치는 앞 절의 step3과 동일한 과정을 진행하되 장치 내 저장된 사용자인증서를 추출하여 authenticatorMakeCredential 메시지 내 authData extension 영역에 저장한다. 사용자인증서는 앞 절의 step4 와 step5 과정에 포함되어 서버로 전송된다. 이를 수신한 서버는 step6 과정에서 FIDO 검증을 마친 후 사용자인증서의 유효성을 검증한다. 검증이 성공하면 DB 에 저장한다. 이 때 인증장치 내부에는 사용자의 인증서와 개인키가 안전한 저장소에 저장되어 있음을 전제로 한다. 인증장치 내 사용자인증서와 개인키를 저장하기 위해서는 별도의 발급 또는 주입과정이 필요하다. 예를 들면 장치 내부에서 공개키쌍을 생성한 후 CMP[24] 나 CRMF[25] 등 표준 프로토콜을 반영하여 저장하거나 외부에서 생성된 사용자인증서와 개인키를 인증장치 제조사가 배포한 프로그램을 통하여 주입시킬 수 있다. 그 밖에도 다양한 방법이 존재할 수 있으므로 본 고에서는 구체적 저장방법에 대한 기술을 생략한다.

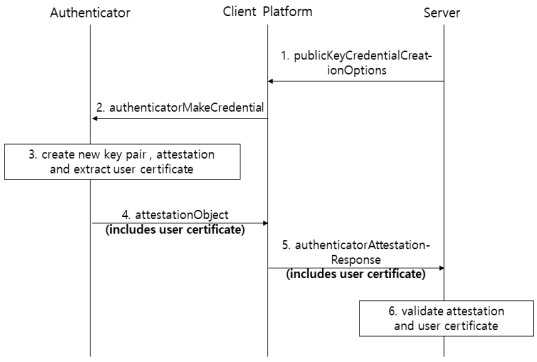

Fig. 7. A method of certificate registration using FIDO2/WebAuthn user flows

3.6.3 FIDO2 인증(authentication)

FIDO2 인증은 사용자가 인증장치를 통하여 생체인증(user verification)을 한 후 서버가 요청한 값에 대한 결과값을 인증장치를 통하여 서버에 제출 및 검증하는 과정이다. 일반적인 FIDO2 인증절차는 다음과 같다.
step1.CP는 서버 접속 후 서버로부터 getAsserton 요청메시지(publicKeyCredentialRequestOptions)를 수신한다. (이 메시지는 서비스 서버의 URL 같은 서버 정보와 서명원문이 포함되며 이 때 서명원문

은 FIDO2 인증장치의 서명을 위한 것이지만 필요에 따라 사용자개인키로 서명할 대상이 될 수 있다.)
step2. CP는 수신한 요청메시지를 인코딩한 후 (authenticatorGetAssertion) 주단말기와 연결된 인증장치에게 전달한다.
step3. 요청메시지를 수신한 인증장치는 생체인증 등 로컬 단에서 사용자를 인증하는 과정(user verification)을 거친 후 FIDO2 등록과정에서 생성한 인증용 비밀키(authentication private key)로 검증에 필요한 값들을 전자서명 한다. 이 값을 포함하여 정의된 보안 파라미터와 함께 assertion 메시지를 생성한다.
step4. 인증장치는 assertion 메시지를 정의된 타입(CBOR)으로 인코딩한 후 CP로 전송한다. (authenticatorGetAsseritionResponse)
step5. 응답메시지를 수신한 브라우저는 적절한 타입으로 메시지를 인코딩 후 서버로 전송한다. (authenticatorAssertionResponse)
step6. 서버는 CP로부터 assertion 메시지를 수신한 후 검증한다.

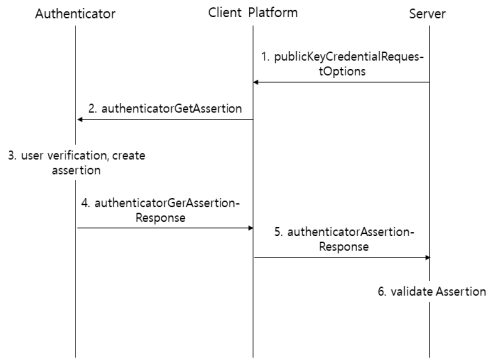

Fig. 8. Basic FIDO2/WebAuthn user flows : FIDO2 Authentication

3.6.4 사용자인증서에 기반한 전자서명

사용자인증서 기반 전자서명 과정은 앞 절 FIDO2 인증과정에 포함된다. step1과 step2는 앞 절과 동일하다. step3에서 인증장치는 앞 절의 step3과 동일한 과정을 진행하되 assertion 을 생성하기 전 사용자인증서 기반 전자서명을 진행한다. 전자서명에 사용된 전자서명 원문은 CP 로부터 전달 받은 authenticatorGetAssertion 에 포함된

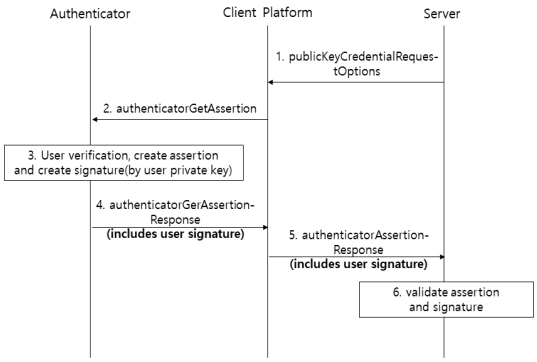

Fig. 9. A method of digital signature and validation through FIDO2/WebAuthn

챌런지(challenge)가 될 수 있다. 생성된 전자서명 값은assertion 메시지 내 확장영역(authData extension)에 저장한다. 사용자인증서 기반 전자서명 값은 앞 절의 step4 와 step5 과정에 포함되어 서버로 전송된다. step6 과정에서 응답메시지(authenticatorAssertionResponse)를 수신한 서버는 메시지 검증 후 확장영역의 전자서명값을 추출하여 검증한다.

3.7 제안모델의 효과

본 제안모델은 FIDO2 표준 프로토콜을 통하여 인증장치 내 저장된 사용자인증서가 서버에 등록될 수 있다는 것과 사용자인증서와 쌍이 되는 개인키의 전자서명이 인증장치에서 생성되어 서버에서 검증될 수 있음을 보인 것이다. 기술한 모든 과정이 웹표준에 위배되지 않으므로 중계역할을 하는 웹브라우저(CP)에는 별도의 플러그인이 설치 될 필요가 없고 모든 스트리밍 데이터에 대하여 어떠한 오류/경고 메시지도 나타나지 않음을 예측할 수 있다. 이러한 예측이 실제와 부합하는지의 여부는 다음 절의 실험을 거쳐 확인하였다. 사용자 관점에서는 인증서의 암호를 입력하거나 기억할 필요가 없어졌고 이에 따른 키보드 보안 프로그램 설치의 불편함도 사라지게 되었다. 또한 인증장치 내 저장된 사용자개인키의 유출이 매우 어려우므로 기존 플러그인을 사용하는 하드디스크 저장 방식의 전자서명에 비해 보안성이 높아졌다. 이러한 보안성의 향상으로 인해 악성코드 탐지 프로그램의 설치 필요성도 현저히 낮아질 것으로 기대된다. (본 모델은 CTAP을 이용한 외부인증장치 연결 방식을 대상으로 한다. 이 외에도 CP 단말에 인증장치

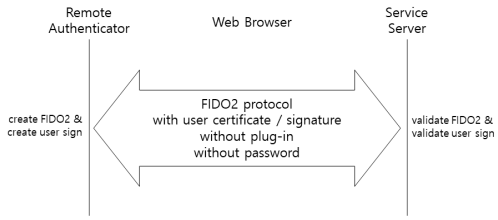

Fig. 10. Diagram of the proposed model

가 탑재(built-in) 된 방식이 있으며 TPM(Trusted Platform Module) 같은 별도의 이용 안전성을 갖추어야 한다[23].)

3.8 유사모델 비교를 통한 제안모델의 우수성

1. 패스워드 입력 여부 : 현재까지 대표적인 인증방법으로 쓰이는 패스워드는 추측, 탈취, 피싱 등의 공격으로부터 취약하며[30] 인터넷 환경이 고도화 됨에 따라 기억하기 어렵고, 규칙이 복잡해졌다. 특히 공인인증서와 같은 사용자인증서와 쌍이 되는 개인키는 패스워드 기반 암호방식[31] 또는 PIN 기반 접근제어 방식[32]을 사용한다. (이 경우 패스워드나 PIN 이 서버 DB 에 저장되지 않고 로컬 단말기에서만 검증하므로 일반 패스워드 기반보다 안전하다 할 수 있지만 이 역시 도용, 유출의 위험이 있다.) FIDO 규격의 가장 중요한 목적 중 하나는 이러한 패스워드를 사용하지 않는 인증(password-less authentication) 으로 FIDO1.0 부터 K-FIDO, FIDO2 까지 지속적으로 패스워드 대체인증 방식의 보안 구조가 설계되어 왔다. 본 제안모델은 FIDO2 를 기반으로 한 외부 생체인증장치 방식이므로 패스워드로 인한 불편함과 취약성을 해결하였다.
2. 사용자인증서 지원방안 : 사용자인증서의 안전한 사용 예로는 보안토큰과 K-FIDO 가 될 수 있다. 둘 다 웹브라우저가 지원하지 않는 규격을 사용하므로 별도의 플러그인을 설치해야 하는 불편함이 따른다. 본 제안모델은 기존의 사용자인증서를 FIDO2 웹표준과 결합하여 사용자개인키의 저장 안전성을 확보한다. 또한 인증서관리, 키보드보안 등을 위한 별도의 프로그램이 필요하지 않는 모델이므로 사용자인증의 보안성과 편의성을 향상시켰다 할 수 있다.
3. 웹표준 지원여부 : 국내 사용자인증 및 전자서명이 필요한 대부분의 웹서비스는 서비스를 인터넷상에서 진행하기 위한 관련기능의 표준 부재로 인하여 인증서관리, 키보드보안, 전자서명, 보안토큰 연동 등의 기능을 제공하기 위하여 플러그인과 같은 별도의 프로그램을 설치해야 하는 불편함이 컸다. 본 모델에는 사용자인증서 및 개인키가 인증장치 내에 있고 CP 와 인증장치의 통신규격(CTAP) 및 이를 서버와 연계될 수 있도록 API(WebAuthn) 가 표준화되어 있다. 또한 패스워드의 입력이 필요 없으므로 관련 플러그인의 설치가 없도록 하였다.
4. 플러그인 설치여부 : 본 모델은 사용자인증서와 연동되는 타 모델 중에서 유일하게 플러그인을 설치하지 않음으로 이용 편의성을 높일 수 있었다.
5. 국제표준 준수 : 본 모델은 ITU-T 및 W3C 에 표준 등재된 FIDO2 규격 내에서 동작하는 구조이므로 국제표준을 준수하게 하였다[2][15]. 따라서 인터넷환경에서 사용자인증서를 안전하게 이용하고자 하는 모든 국가들이 쉽게 구현할 수 있는 모델이다.
6. 상호연동성 : 본 모델은 한 번 발급받으면 동일한 인증서로 대부분의 인증사이트를 이용할 수 있는 공인인증서와 동일한 효과를 가진다. 사용자는 서비스 사이트별로 인증서 등록과정만 거치면 해당 서비스를 이용할 수 있다.
7. 부인방지효과 : 전자계약, 전자상거래 등 공정한 거래임을 확인해야 하는 서비스에는 부인방지(특히 사용자의 거래 내역 부인을 방지) 기능이 반드시 필요하다[33]. PKI 상에서의 표준 전자서명[34]은 서명 당사자의 서명 내용 부인을 방지시키는 대표적인 메커니즘이며 국내에서는 전자서명법과 사용자인증서를 활용하여 이를 실현해 왔다. 본 모델에서의 부인방지효과는 첫째 사용자인증서 전자서명을 함으로써 기존과 동일한 수준의 부인방지 효과를 가질 수 있으며 둘째 FIDO2 인증 과정에서 인증장치의 기기인증서 비밀키로 서버가 전송한 원문을 서명함으로써 부인방지 효과를 높일 수 있으며 셋째 사용자 전자서명용 키가 인증장치 내 유출이 어려운 공간에 저장되어 공인인증서 보안토큰의 역할을 함으로써 키소유의 유일성과 안전성을 높일 수 있다. 마지막으로 본 모델이 포함하는 FIDO2 에서의 전자서명에서 서명원문은 서버에서 생성하여 CP 로 전송하고 CP 는 자신의 정보를 원문에 추가하여 메모리해킹과 같은 원문의 위조를 매우 어렵게 하였다. 이와 같이 본 모델은 FIDO2 와 사용자인증서의 장점을 취함으로써 부인방지 효과를 기존방식에 비해 매우 높일 수 있게 되었다.

Table 1. Function comparison of each model

	User Cert	FIDO 1.0	K-FIDO	FIDO2	Propo-sed Model
password-less	X	O	O	O	O
support user certificate	O	X	O	X	O
support web standard	X	O	X	O	O
non plug-in	X	X	X	X	O
global standard	X	O	X	O	O
interoper-ability	O	X	X	X	O
non-repudiation	O	△	O	△	O

IV. 실험 및 결과

4.1 실험 시스템 구성

본 제안모델의 검증을 위하여 실험시스템은 인증장치(Test Authenticator)와 CP와 검증서버(Test Server)로 구성된다. 인증장치와 검증서버는 본 실험을 위하여 직접 구현된 것이며 CP 는 업무용으로 많이 쓰는 데스크톱 PC 에 Windows , Internet Explorer 와 같은 범용 운영체제 및 브라우저를 조합하여 실험하였다.

4.1.1 인증장치

실험에 사용한 인증장치는 지문동글형(fingerprint dongle type) 외부 인증장치이며 FIDO2 CTAP 및 제안모델이 구현되었다. 인증장치는 PC 의 USB 포트와 연결되어 USB 표준 인터페이스인 HID[28] 및 FIDO2 CTAP 프로토콜로 PC 와 송수신을 진행한다. 인증장치 내부에는 프로그램 동작을 위한 마이크로칩 및 플래시메모리 및 안전한 저장소(secure element) 등으로 구성되어 있다. 인증장치 프로그램은 펌웨어 형태로 탑재되며 HID, CTAP, CBOR인코더, 공개키연산/전자서명(crypto) 및 로그 기능이 구현되어 있다. 또한 본 제안모델을 실험하기 위한 사용자인증서가 저장되어 있다.

Table 2. Specification of the Authenticator

contests	spec.
chip operating system	COMET504
	JavaCard v2.2.1
	GP/VGP v2.1.1
secure element	STMicroelectronics
	ST31G480
protocol type	CTAP2
algorithm	ECDSA_256
	SHA256
	AES256

4.1.2 CP (Client Platform)

CP 는 FIDO2 규격에서 정의 되었으며 FIDO2 클라이언트 역할을 하는 장치 및 프로그램을 의미한다. 본 실험에서의 CP 는 PC , 운영체제, 웹브라우저로 구성되며 각각의 종류를 조합하여 실험을 하였다. 운영체제는 Windows10 / Windows7 및 Mac (v10.14)를 대상으로 하였으며 각각에 대하여 Edge, Internet Explorer 의 최신버전 및, Chrome(70) 웹브라우저를 사용하였다. CP 는 HID, FIDO2 CTAP , WebAuthn API 등 기술한 국제표준 규격들이 구현되어 있다. 본 실험에서는 CP에서 지원하는 웹표준 기능만을 사용하므로 플러그인 등 별도의 프로그램 설치 없이 진행 하였다.

4.1.3 검증서버 (Test Server)

검증서버는 FIDO2 검증기능을 포함하고 테스트용 페이지를 제공한다. 사용자인증서와 전자서명 값을 FIDO2 메시지 extension으로부터 추출하여 분석하는 기능을 포함한다.

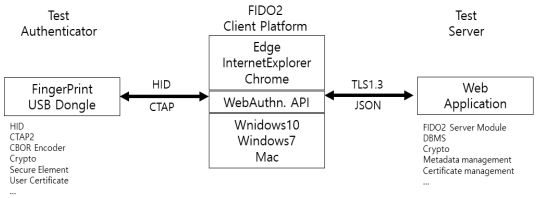

Fig. 11. Protocol overview of the proposed model

4.2 실험방법

본 실험에서 입증하고자 하는 것은 인증장치에서 생성한 메시지가 클라이언트 단말로 전송될 때 클라이언트 플랫폼 및 웹브라우저에서 아무 오류 메시지

없이 서버로 전송(bypass) 되는 프로세스이다. 따라서 본 모델에서 제안하는 개념을 유지하는 범위에서 제한된 실험을 하였다. (CP 와 검증서버와의 통신보안은 TLS1.3 을 적용하였고 메시지 형식은 JSON 타입으로 인코딩 하였다.) 실험환경은 Windows7, Windows10, Mac 플랫폼과 Internet Explorer, Edge, Chrome 브라우저를 대상으로 조합하여 진행하였다. 테스트를 위한 페이지는 WebAuthn API를 반영한 간단한 스크립트로 구현되었다[15].

4.2.1 인증서 등록

makeCredential message 내 authData extension 위치에 인증장치 내 저장된 사용자인증서 데이터를 추가한 후 PC 로 전송하여 이를 FIDO 서버가 수신하는 과정이다(Fig.7). 인증서 등록 실험 절차는 3.6.2 절에 기술한 제안모델과 동일하다.

- 인증장치 내 저장된 사용자 인증서는 DER[36] 인코딩 되어진 x.509[35] 형식의 테스트 인증서이다(Table 3 : No. 3).
- 인증장치에서 CP(웹브라우저) 로 전달되는 데이터는 CTAP 규격에 의해 CBOR 로 인코딩 되어진다(Table 3 : No. 1, No. 2).
- CBOR 데이터를 수신 받은 CP는 WebAuthn. API를 호출하여 JSON 타입으로 변환, 서버로 전송한다(Table 3 - No. 4, No. 5).

4.2.2 전자서명

getAssertion message 내 authData extension 위치에 정적데이터를 추가한 후 PC 로 전송하여 이를 FIDO 서버가 수신하는 과정이다(Fig.9). 전자서명 실험 절차는 3.6.4 절에 기술한 제안모델과 동일하다. 이 때 정적데이터는 임의로 정한 값이며 런타임에서 생성된 전자서명값을 의미한다. 본 실험에서는 인증장치가 포함한 정적데이터가 오류없이 웹브라우저를 거쳐 서버에 전송되고 서버는 메시지 디코딩 과정에서 이 값을 추출하여 출력함을 확인한다.

Table 3. Test vectors and sample code

No.	Data
1	A3 # map(3) 01 # unsigned(1) 66 # text(6) 7061636B6564 # "packed" 02 # unsigned(2) 59 091D # bytes(2333)
2	DCB8470466F2B8D10383198F601759F6BC3455146A2A0C58033C4BA84844F0B6C50000000011234567820190520527 7AD44F139A75700E0C90C50C3A0B5F362549F9263FE3972DBDDCE5969F31C57C7A189D74495374D172BCF603CCB899705147FC7977EDC43629EB0373A2A06027862C200900E4A26480985DE364DEACEFBB5ADB4F0536318...
3	DB₩x16₩xD9z5₩xA1dNPKly₩a₩xB0MIIFwDCCBKigAwIBAgIDfsApMA0GCSqGSIb3DQEBCwUAME8xCzAJBgNVBAYTAktSMRIwEAYDVQQKDAlDcm9zc0NlcnQxFTATBgNVBAsMDEFjY3JlZGl0ZWRDQTEVMBMGA1UEAwwMQ3Jvc3NDZXJ0Q0EyMB4XDTE1MDgyODAzMjcwMFoXDTE2MDkxOTE0NTk1OVowejELMAkGA1UEBhMCS1IxEjAQBgNVBAoMCUNyb3NzQ2VydDEVMBMGA1UECwwMQWNjc...

4	let tests = {
	'makeCredential': () => {
	let attestation = 'direct';
	var strName = document.getElementById('identifierId').value;
	var arrN = strName.split('@');
	window.displayName = arrN[0];
	window.username = document.getElementById('identifierId').value;
	return getChallenge('attestation', {displayName, username, attestation}).then((response) => {
	let publicKey = preformatMakeCredReq(response);
	return navigator.credentials.create({ publicKey })
	})
	.then((response) => {
	let makeCredResponse = publicKeyCredentialToJSON(response);
	return sendWebAuthnResponse('attestation', makeCredResponse)
	}) ...

5	'getAssertion': () => {
	var strName = document.getElementById('identifierId').value;
	var arrN = strName.split('@');
	window.displayName = arrN[0];
	window.username = document.getElementById('identifierId').value;
	return getChallenge('assertion', {displayName, username})
	.then((response) => {
	let publicKey = preformatGetAssertReq(response);
	return navigator.credentials.get({ publicKey })
	}).then((response) => {
	let makeCredResponse = publicKeyCredentialToJSON(response);
	return sendWebAuthnResponse('assertion', makeCredResponse)
	})
	}

4.3 실험결과

실험결과는 현재 FIDO2 WebAuthn API 가 반영되지 않은 일부 브라우저를 제외하고 오류 없이 인증장치 메시지가 서버로 전송되었다. 서버는 FIDO2 메시지를 수신한 후 extension buffer 의 내용을 인증장치에서 생성한 내용과 같은지 바이너리 값 비교를 거쳤다.

Table 4. Data received by server : registration

Data received from client platform

// JSON received
Authenticator data : {
"fmt":"packed",
"attStmt":{
"alg":-7,
 	
"sig":"MEQCIBhfAot5yUk/wrB89MklWfWqEIoUHkBztLV7S3h5VLbEAiAR64HmzZAUedpJpzPlo21dhAUnWxsRTpTElvZP10eYQg==",
 	
"x5c":["MIIB3zCCAYagAwIBAgIJAMbKETDOSyiTMAoGCCqGSM49BAMCMDgxCzAJBgNVBAYTAktSMQwwCgYDVQQKDANZS0sxDjAMBgNVBAsMBUZJRE8yMQswCQYDVQQDDAJDQTAeFw0xOTA1MjAwNzQ1...
 	
"authData":"SZYN5YgOjGh0NBcPZHZgW4/krrmihjLHmVzzuoMdl2PFAAAAARI0VnggGQUgUnetRPE5p1cA4BkOBSrLeqdIU8aGjG2CXWpM3JFASiyZex0ZVaqp9Q0yFomNoIi0z9vJogAFae0zS3xPfkbOrELS1I3trICmdz0RWyfS2J...3ssbTtbSGkITv6vR+QHIHnC/0QA6uAqiIlggtIndOXa2jmrN+pkUY6vTO64cmr4nzfX8CGMTi4mW/CWhZE5QS0lxZmFhZGxrZmphc2xkZmFzZGY="
}
 	
RPIDHASH hex :
49960de5880e8c687434170f6476605b8fe4aeb9a28632c7995cf3ba831d9763
FLAGS hex : c5
COUNTERS hex : 00000001
extensionsBuffer : 4Vx ▯ ▯ Rw◆D◆9◆W
AAGUID hex : 123456782019052052 77ad44f139a757
...

Table 5. Extraction of extension data : registration

Data
// Parse and Verify INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - AuthData length : 2349 INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - flagsBuffer : c5 INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - hasAtFlag : true INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - hasExtensionsFlag : true INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - COUNTERS hex : 00000001 INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - cosePublicKey size: 2054 INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - leftovers size: 1977 INFO : com.ydentity.cmm.fido2.service.CommonVerifiers - NPKI : MIIFwDCCBKigAwIBAgIDfsApMA0GCSqGSIb3DQEBCwUAME8xCzAJBgNVBAYTAktSMRIwEAYDVQQKDAlDcm9zc0NlcnQxFTATBgNVBAsMDEFjY3JlZGl0ZWRDQTEVMBMGA1UEAwwMQ3Jvc3NDZXJ0Q0EyMB4XDTE1MDgyOJ3dJiZFIkut8iwpgOh6tAgqna7YCq1W1XE6BN1RAPoulHkWnxf2r7B3fuH09yJ8iDnTVyzdFlh5vaD2UfhwiPLdhdLs4t8A/LHAE731QQvcF+Cq4HAIl... INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - extensionsBuffer : ... INFO : com.ydentity.cmm.fido2.service.AuthenticatorDataParser - extensionsBuffer size: 1977 WARN : com.ydentity.cmm.fido2.service.processors.PackedAttestationProcessor - OID (id-fido-gen-ce-aaguid) not exist INFO : com.ydentity.cmm.fido2.attestation.AttestationService - registerationResponse result : {"errorMessage":"","status":"ok" } Request URL::http://localhost:8080/webauthn/attestation/result Sent to Handler :: Current Time=1569561143893

Linux 계열 운영체제와 Firefox, Opera 브라우저는 실험대상에서 제외하였고 Windows 7, Windows 10, Mac 운영체제를 대상으로 실시되었다. Chrome 브라우저는 3개 OS를 모두 지원하여 호환성이 가장 높았으며 Internet Explorer 는 FIDO2 기능이 탑재되지 않음을 알 수 있다. 나머지 항목에서 실험결과는 제안모델의 예상 결과와 일치했다. 본 실험에서는 사용자인증서의 전자서명을 실제 연산하지는 않았으므로 이에 대한 성능지연은 논외로 한다. 단, FIDO2 등록과 인증과정에서 발생하는 기기 전자서명에 대한 지연시간은 본 인증장치 기준으로 500ms 미만이며 이를 감안할 때 사용자인증서 전자서명에 의하여 추가로 발생하는 시간지연은 실 서비스 운영에 영향을 미칠 정도의 크기는 아닐 것으로 예상된다.

Table 6. Result of the FIDO2 interoperability test

OS	Browser	registration	user digital sign
Windows 10	edge	success	success
	chrome	success	success
	i.e.	N/A	
Windows 7	chrome	success	success
	i.e.	N/A	
Mac OS	chrome	success	success
	safari	N/A	

V. 결론 및 향후과제

본 논문에서는 W3C WebAuthn 표준과 FIDO2 규격을 활용하여 공인인증서와 같은 사용자인증서 전자서명이 웹브라우저 상에서 프로그램이나 플러그인 설치 없이 진행될 수 있음을 확인하였다. 이는 FIDO2 CTAP 규격의 확장영역(extension) 을 웹브라우저의 클라이언트 플랫폼에서 오류를 발생시키지 않는 속성을 활용한 것이다.

본 제안모델은 현행 공인인증서(또는 사용자인증서)의 일반적인 이용방법과 FIDO2 표준의 특성을 결합하여 웹표준에 부합할 뿐 아니라 편의성을 크게 높였다는데 의미가 있다. FIDO 의 등장으로 기존 공인인증서 이용환경의 문제점을 해결하려는 시도는 FIDO1.0 UAF, K-FIDO, FIDO2를 거쳐 여러 번 있었으나 각각의 한계를 극복하기 어려웠다. 본 제안모델을 통하여 그 동안 극복하기 어려웠던 플러그인 설치의 문제를 해결하였으며 부차적인 요소들도 해결되었다(Table 1). 초연결사회가 도래하면서

서비스 이용 주체 인증의 중요성이 보다 강조되고 있을 뿐만 아니라 생체인증을 비롯한 다양한 인증방식의 요구가 커지고 있다. 이를테면 휴대폰과 PC 가 BLE 통신으로 인증을 하거나 휴대용 지문동글 인증장치 활용도 가능해 졌으며 기존 공인인증서를 생체인증과 결합하여 재활용하는 요구도 있을 수 있다. 이렇듯 다양한 인증방식은 본 제안모델과 실험을 통하여 구현 가능함이 입증되었으며 향후 급속히 성장하는 차세대인증 시장에 큰 파급력을 줄 것으로 기대된다. 실험과정은 실제 생성한 전자서명값 대신 임의의 정적데이터로 진행한 제한적인 방법을 썼고 향후에는 보다 실증적 검증을 하기 위하여 다양한 알고리즘을 탑재하여 진행할 필요가 있다. 또한 FIDO2 CTAP extension 은 사용자 인증장치와 서버 간 정의 가능한 프로토콜 영역이므로 전자서명 뿐 아니라 OTP 나 장치를 이용한 암복호 기능 등 향후 다양한 연구와 실험을 진행할 예정이다.

References

[1] ITU-T, "Universal authentication framework," X.1277(11/2018) , SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cyberspace security - Identity management, Sep. 2018.

[2] ITU-T, "Client to authenticator protocol/Universal 2-factor framework," X.1278(11/2018) , SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Cyberspace security - Identity management, Sep. 2018.

[3] Jang, S. S., "A Study on the Effect Fintech on the Information Security Industry," Internet & Security Focus, pp. 4-32, Mar. 2015.

[4] Jae-Hun Song and In-Seok Kim, "A Study on the Utilization of Biometric Authentication for Digital Signature in Electronic Financial Transactions: Technological and Legal Aspect," The Journal of Society for e-Business Studies, 21(4), pp.41-53, Nov. 2016,

[5] Korea Internet & Security Agency, "Implementation Guideline for Safe Usage of Accredited Certificate using bio information in Smart phone," KCAC.TG.IMP, Sep. 2016.

[6] Byoungcheon Lee, "Certified Key Management in Multi K-FIDO Device Environment," Journal of the Korea Institute of Information Security and Cryptology, 30 Apr. 2017.

[7] Daehak Kim, "On the application of authorized certificate for cryptology," Journal of the Korean Data And Information Science Society 28(1), pp. 163-171, Jan. 2017.

[8] FIDO Alliance, "FIDO Security Reference," https://fidoalliance.org/specs/fido-u2f-v1.0-ps-20141009/fido-security-ref-ps-20141009.html, Oct. 2014.

[9] Electronics and Telecommunications Research Institute, "User Authentication Method and Apparatus Using Digital Certificate on FIDO 2.0 Method Thereof," Mar. 2018.

[10] Kyung-Hye Park, "A Study of the scenario for improvement of NPKI system," Journal of Digital Convergence, pp. 59-71, Nov. 2010.

[11] Jeong Gi Seog, "A Study on Measures for Improving Obligatory Use of Digital Certificate for Eletronic Financial Transactions," Journal of Digital Convergence, pp. 25-33, Dec. 2013.

[12] Anna Angelogianni, "ANALYSIS AND IMPLEMENTATION OF THE FIDO PROTOCOL IN A TRUSTED ENVIRONMENT," M.Sc. Digital Systems Security, pp. 9-43, Jun. 2018

[13] Chae, Cheol Joo, "Authentication Method using Multiple Biometric Information in FIDO Environment," Journal of Digital Convergence, pp. 159-164, Jan. 2018.

[14] FIDO alliance, "FIDO UAF Protocol

Specification v1.0," https://fidoalliance.org/specs/fido-uaf-v1.0-ps-20141208/fido-uaf-protocol-v1.0-ps-20141208.html, Dec. 2014.
〔15〕 W3C, "Web Authentication: An API for accessing Public Key Credentials Level 1," https://www.w3.org/TR/webauthn/, W3C Recommendation, Mar. 2019.
〔16〕 Kim-jun Woo, "Study on The Prevention of User Authentication Information Reuse : Focusing on Electronic-Signature," Jan. 2019.
〔17〕 FIDO alliance, "Universal 2nd Factor (U2F) Overview," https://fidoalliance.org/specs/fido-u2f-v1.2-ps-20170411/fido-u2f-overview-v1.2-ps-20170411.html , Apr. 2017.
〔18〕 Seongjin Lee, Donghyun Choi, Dongho Won, Seungjoo Kim, "International PKI Construction Status Analysis," Korea Institute Of Information Security And Cryptology, pp. 2-14, Dec. 2007.
〔19〕 IEEE, "An overview of PKI trust models," IEEE Network Network, IEEE. vol. 13, no. 6, pp. 38-43 Jan, 1999.
〔20〕 Jae Jung Kim, Seng 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, Nov. 2016
〔21〕 IETF, "The Transport Layer Security (TLS) Protocol Version 1.3," Request for Comments: 8446, Aug. 2018.
〔22〕 S. Durce et al., "S/MIME Version 2 Merwge Specikalion.," Request for Comments: 231, Mar. 1998.
〔23〕 FIDO alliance, "FIDO2.0 : Key Attestation Format," https://fidoalliance.org/specs/fido-v2.0-ps-20150904/fido-key-attestation-v2.0-ps-20150904.html, FIDO Alliance Proposed Standard, Apr. 2015.
〔24〕 IETF, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)," Request for Comments: 4210, Sep. 2005.
〔25〕 IETF, "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)," Request for Comments: 4211, Sep. 2005.
〔26〕 National Information Society Agency, "NATIONAL INFORMATIZATION WHITE PAPER," ISBN : 978-89-8483-363-0, pp. 4-10, Nov. 2018.
〔27〕 Korea Internet & Security Agency, "Introduntion of Accredited Certification Service," https://www.rootca.or.kr/kor/accredited/accredited03_05.jsp, Aug. 2019.
〔28〕 Mike Bergman et al., "Device Class Definition for Human Interface Devices (HID)," USB Implementers' Forum, Firmware Specification-6/27/01, Version 1.11, Jun. 2000.
〔29〕 IETF, "Concise Binary Object Representation (CBOR)," Request for Comments: 7049, Oct. 2013.
〔30〕 Hong Gi Kim and Im Yeong Lee, "A Study on One-Time Password Authentication Scheme in Mobile Environment," Journal of Korea Multimedia Society, 14(6), pp. 785-793, Jun. 2011.
〔31〕 RSA Data Security Inc., "PKCS #5: Password-Based Cryptography Specification Version 2.0," Request for Comments: 5652, Sep. 2010.
〔32〕 RSA Data Security Inc., "PKCS #11 v2.11 : Cryptographic Token Interface Standard.," Nov. 2001.
〔33〕 Moonseog Seo et al., "On the Standard Mechanism for Non-repudiation Services," Information and Communications Univ, Dec. 2010.

〔34〕 RSA Data Security Inc., "Cryptographic Message Syntax (CMS)," Request for Comments: 5652, pp. 6-17, Sep. 2009.
〔35〕 IETF, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," Request for Comments: 5280, May. 2008.
〔36〕 Burton S. Kaliski Jr., "A Layman's Guide to a Subset of ASN.1, BER, and DER," An RSA Laboratories Technical Note, Nov. 1993.
〔37〕 FIDO alliance, "Specifications Overviews," https://fidoalliance.org/specifications/, Aug. 2019.

〈저자소개〉

조 한 구 (Hankoo Cho) 종신회원
1997년 2월: 경희대학교 물리학과 학사
2016년 2월: 고려대학교 정보보호대학원 정보보호학과 석사
2015년 9월~현재: 주식회사 와이키키소프트 대표이사
〈관심분야〉 암호, 인증, AI
E-mail: hkcho@whykeykey.com

이 경 호 (Kyung-ho Lee) 종신회원
1989년 8월: 서강대학교 수학과 학사
1997년 8월: 서강대학교 정보통신대학원 석사
2009년 8월: 고려대학교 정보보호대학원 박사
1994년 2월: 삼성그룹, 네이버(주), 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책
E-mail: kevinlee@korea.ac.kr