정 보 보 호 학 회 지
제26권 제2호, 2016. 4

FIDO 2.0 범용인증기술 소개

조 상 래*, 조 영 섭*, 김 수 형*

요 약

국내 인증기술은 패스워드를 시작으로 X.509 인증서 기반의 공인인증 기술로 발전되어 왔고 현재는 패스워드의 보안 취약성을 개선하기 위해 개발된 FIDO 기술로 전환되는 과정에 있다. FIDO는 바이오 인증 기술뿐만 아니라 다중 인증 기술도 지원하는 범용인증기술로 FIDO 인증 서버를 한번만 설치하면 서비스 제공자의 요구사항에 따라 다양한 인증방식을 서버 변경 없이 수용할 수 있다는 장점을 가지고 있어, 금융, 결제 등 다양한 분야에 급속하게 확산되고 있다. 본 고에서는 범용인증기술인 FIDO 1.0 기술을 설명하고 최근에 표준화를 진행하고 있는 FIDO 2.0 기술에 대한 소개 및 FIDO 1.0 기술과의 차이점을 기술하여 FIDO 2.0이 가지는 여러 의미를 분석하여 향후 인증기술에 대한 전망을 제시한다.

Ⅰ. 서 론

국내 인증기술은 패스워드를 시작으로 X.509 인증서를 기반으로 하는 공인인증 기술로 발전되어왔다. 패스워드는 간편하게 사용할 수 있는 사용자 인증기술이지만 보안에 취약하고 외부 유출 가능성이 높고 해킹에도 취약하다는 단점이 있다. 그러나 사용이 편하고 운영하는데 비용이 거의 들지 않아 지금도 많은 웹사이트에서 사용자 인증 기술로 사용되고 있다.

2000년 인터넷 뱅킹 서비스를 제공하기 위하여 전자서명법이 발효되고 국내에 공인인증 기술이 도입되었다. 공인인증 기술은 공개키기반구조를 이용하는 강력한 인증 기술로 보안상 취약점이 적고 부인방지 기능을 제공하여 온라인 금융거래의 요건을 만족하는 기술로 국내에 널리 보급되고 사용되어 왔다. 그러나 최근 공인인증기술이 가지는 ActiveX를 이용한 웹서비스의 보안 취약성 문제와 모바일환경에서의 사용 불편함이 부각되면서 새로운 대체 인증기술의 도입의 필요성이 높아지고 있는 실정이다.

사용자 인증을 위해 사용되는 인증 방식들은 크게 지식기반, 소유기반, 생체기반으로 구분되며 각 인증 방식은 사용자 편의성, 보안성 등에서 차이점을 가지고 있다. 현재 국내에서 사용되는 인증기술은 패스워드를 이용하는 지식기반을 시작으로 공인인증서를 사용하는 소유기반을 거쳐 지문인식과 같은 생체기반으로 이동하고 있다. 기술의 발전과 생체 인증장치의 보편화에 따라 사용자의 생체 정보를 기반으로 하는 인증 방법은 향후 보편적으로 사용될 것으로 예상되며 이를 위해서는 다양한 생체 인증 방법을 수용할 수 있는 범용 인증 기술이 반드시 필요하다[7].

FIDO는 패스워드를 제외한 모든 인증방식을 사용할 수 있는 범용 인증 기술로 FIDO 인증 서버를 한번만 설치하면 인증장치를 서비스 제공자의 요구사항에 맞게 얼마든지 변경이 가능한 구조로 설계되어 바이오 인증 기술뿐만 아니라 다중 인증 기술도 지원한다.

본 고에서는 범용인증기술인 FIDO 1.0 기술을 소개하고 최근에 표준화를 진행하고 있는 FIDO 2.0 기술에 대한 소개 및 FIDO 1.0 기술과의 차이점을 기술한다.

Ⅱ. FIDO Alliance 소개

본 장에서는 FIDO Alliance의 연혁과 기 개발된 그리고 현재 개발 중인 표준규격에 대하여 기술한다.

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발 사업의 일환으로 하였음 [B0126-15-1007, "상황인지 기반 멀티팩터 인증 및 전자서명을 제공하는 범용 인증 플랫폼 기술 개발"].
* 한국전자통신연구원 인증기술연구실 (sangrae@etri.re.kr, yscho@etri.re.kr, lifewsky@etri.re.kr)

2.1. FIDO Alliance 역사

FIDO(Fast IDentity Online) Alliance는 2012년 여름 결성하여 2013년 2월에 정식으로 출범하였다. FIDO Alliance는 온라인 환경에서 보다 편리하고 안전한 인증 시스템을 공동으로 구축하고 인증 시스템에 대한 기술 표준을 제시하는 역할을 수행하는 연합체이다. 2012년 4월에 Google이 가입하면서 본격적으로 산업계 표준으로 자리를 잡았고 2014년 12월에 FIDO 표준 버전 1.0을 완성하여 발표하였다.

현재 Google, Lenovo, Visa, Master Card, PayPal 등의 250개가 넘는 기업체들이 회원으로 가입하고 있다. 이사회는 29개 업체에 구성되고 한국 기업으로는 삼성전자, 비씨카드 그리고 크루셜텍이 속해 있다. 그 외에 스폰서로 가입한 회사들이 71개 업체이고 관계기업(Associate) 등급으로 구분된 150개 기업들이 참여하고 있다.

2.2. FIDO에서 추진 중인 표준

FIDO는 현재까지 2가지 표준을 제정하여 2014년 12월에 공개하였다. 첫 번째는 웹에서 패스워드를 이용하여 로그인하는 경우에 추가 인증방법으로 보안토큰을 사용하는 U2F(Universal 2nd Factor) 기술이다. 패스워드만 사용하는 웹사이트에서 사용자 인증의 보안성을 높일 수 있는 기술이다.

두 번째는 UAF(Universal Authentication Factor)로 보안성이 취약한 패스워드 대신 지문, 얼굴 등 생체인식과 스마트폰 잠금해제 패턴, H/W 칩 등 강력한 인증 수단을 사용할 수 있는 인증 및 전자서명 기술이다. 스마트폰 등 이용자 단말기에서 생체인증 수단으로 이용자를 인증한 후 서비스 제공자 서버와는 공개키 방식으로 원격인증을 수행한다.

FIDO UAF 기술의 동작방식을 살펴보면, 서비스제공자가 원하는 인증장치의 등록을 요청하면 사용자는 해당 인증장치로 로컬인증을 수행하고 공개키를 생성하여 서비스제공자에게 보내 인증장치의 등록을 완료한다. 이렇게 인증장치가 등록된 후 서비스제공자가 인증을 요청하면 등록된 인증장치를 이용하여 사용자를 로컬 인증한다. 로컬 인증으로 사용자가 인증장치에서 확인되면 인증장치는 등록된 비밀키를 접근하여 전자서명 메시지를 생성하고 이를 서비스제공자에게 보내 사용자를 인증하게 된다.

이 기술을 적용하면 사용자는 다양한 인증 수단을 편리하게 사용할 수 있고, 서비스 제공자는 여러 인증 수단을 추가적인 투자나 서버 변경 없이 수용할 수 있게 된다. 이러한 보안성과 개방성을 특징으로 하는 FIDO 인증 기술은 글로벌 기업들이 지금까지 사이버 범죄 대응을 위해 이상거래탐지(Fraud Detection)에 의존하고 이용자 인증은 간편하게 패스워드만 요구해온 흐름에서 벗어나 다양한 수단으로 사용자 인증을 강화하는 추세로 전환하고 있음을 시사해준다.

마지막으로 U2F와 UAF를 통합하여 모든 플랫폼에서 사용할 수 있는 단일 범용인증기술인 FIDO 2.0 표준이 있다. FIDO 2.0은 기술규격 작업은 거의 완료된 상태이고 W3C(World Wide Web Consortium)에서 2016년 말 표준제정을 목표로 표준화 작업을 진행하고 있다.

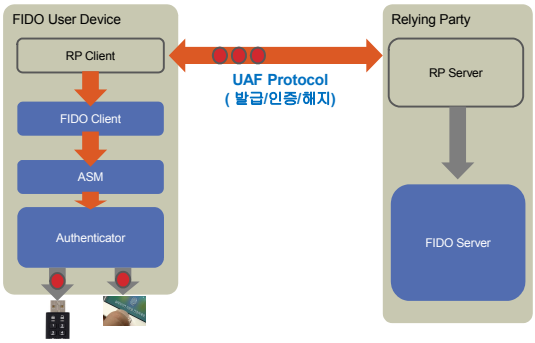
FIDO에서는 관련 기술 표준안을 제정하고, 상호연동시험을 통해 FIDO 규격에 적합한 제품에 “FIDO Certified” 마크를 부여하는 활동을 하고 있다. FIDO 표준 규격을 만족하는 제품들끼리는 어느 나라 제품이던 서로 연동할 수 있다. 예를 들어 국내 스마트폰 이용자가 지문인증을 통해 해외 쇼핑몰의 결제를 할 수 있게 되는 것이다.

Ⅲ. FIDO 2.0 구조

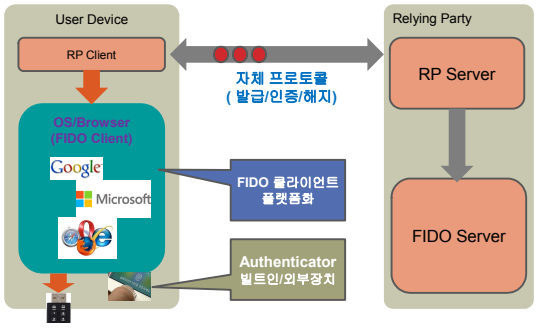
본 장에서는 FIDO 1.0 범용인증기술인 UAF와 FIDO 2.0 기술에 대한 구조를 소개하고 FIDO 2.0에서 변경되는 부분을 설명한다.

3.1. FIDO 1.0 구조 소개

FIDO 2.0 구조를 설명하기에 앞서 FIDO 1.0 구조를 먼저 설명한다. 그림 1은 FIDO 1.0 구조를 도식화한 것이다. 그림에서 FIDO 서버와 FIDO 클라이언트는 응용 서비스에서 제공하는 서버와 클라이언트를 거쳐서 메시지를 주고받는다. 응용 서버는 RP(Relying Party) 서버라고 하고 응용 서비스 클라이언트는 RP 클라이언트라고 부른다. FIDO 서버가 보내는 요청 메시지는 RP 서버에게 전달되고 네트워크를 통해 RP 클라이언트를



〔그림 1〕 FIDO 1.0 시스템 구조



〔그림 2〕 FIDO 2.0 시스템 구조

거쳐 최종적으로 FIDO 클라이언트에 도달한다. FIDO 서버에서 FIDO 클라이언트까지 주고받는 메시지 포맷은 UAF Protocol을 사용한다.

RP 클라이언트에서 FIDO 클라이언트는 안드로이드 운영체제의 경우에는 Intent라는 내부 프로세스 통신규칙을 따라 호출되고 호출하는 규격은 FIDO 표준규격에 명시되어 있다. FIDO 클라이언트와 ASM(Authenticator Specific Module)이 통신하는 방법도 이와 유사하며 표준에 명시된 별도의 메시지 규격을 사용한다. 인증장치는 보통 하드웨어로 구성되고 소프트웨어도 가능하다.

ASM은 인증장치와 FIDO 클라이언트 간의 소통을 가능하게 하는 디바이스 드라이버라고 생각할 수 있다. ASM은 기본적으로 인증장치를 제조하는 곳에서 제공하는 것으로 FIDO에서 제시하는 개발 가이드라인을 준용해도 되고 자체적으로 개발하여도 무방하다.

FIDO 1.0 표준은 현재 Attestation Certificate를 발급하는 PrivacyCA와 DAA (Direct Anonymous Attestation)을 지원하는 1.3 버전까지 표준규격이 개발되어 있다.

3.2. FIDO 2.0 구조 소개

FIDO 2.0은 FIDO 클라이언트와 ASM을 플랫폼에서 제공하는 것을 목적으로 개발되는 범용인증기술 표준 규격이다. 플랫폼은 크게 윈도우와 안드로이드를 포함하는 운영체제 플랫폼과 웹브라우저를 기반으로 하는 웹 플랫폼을 의미한다.

FIDO 서버, RP 서버와 RP 클라이언트는 서버에서 제공해야 하는 컴포넌트로 서버파트로 생각하면 더 이상 표준 프로토콜이 필요하지 않게 된다. 따라서 FIDO 2.0에서는 UAF Protocol을 사용하지 않고 서버에서 정의하는 자체 프로토콜을 사용하여 메시지를 주고받는다. 기존 FIDO 1.0에서 안드로이드 앱으로 제공되었던 FIDO 클라이언트는 운영체제에서 API로 제공될 예정이며 웹브라우저에서는 자바스크립트 API로 제공된다.

인증장치는 두 가지 종류로 구분한다. 사용자 단말기에 내장되어 있는 빌트인 인증장치와 외부에서 연결되어 동작하는 외부 인증장치로 구분된다. 빌트인 인증장치는 이미 플랫폼 회사와 사전협약을 맺고 개발되기 때문에 표준 규격이 필요 없다. USB, WiFi, NFC 또는 BLE 등을 사용하는 외부 인증장치에 대해서는 FIDO에서 별도의 규격을 개발할 계획으로 있다.

정리하면, 기존에 사용하던 UAF Protocol은 FIDO 서버업체에서 제공하는 자체프로토콜로 대체하며 FIDO 클라이언트와 ASM은 플랫폼에서 제공되어 API가 공개되면 FIDO 응용 개발시에 사용하면 된다. 또한 빌트인 인증장치 개발업체를 제외하면 외부 인증장치 프로토콜을 준용하여 개발하되 FIDO 2.0에서 변경된 전자서명 및 Attestation 포맷을 적용하여야 한다.

FIDO 2.0은 하위 호환성을 지원하지 않을 계획이었으나 현재 1.0 프로토콜을 이용하여 2.0을 지원하는 방안도 논의되고 있어 1.0과 2.0간의 호환성 문제는 당분간 추이를 지켜볼 필요가 있다.

Ⅳ. FIDO 2.0 인증장치

본 장에서는 FIDO 2.0 인증장치가 제공하는 API, 서명 방식 및 인증장치 Attestation 방식에 대하여 기술한다.

4.1. FIDO 2.0 인증장치 API

FIDO 2.0 인증장치는 FIDO 클라이언트에게 다음 세 가지 연산을 제공한다[4].

- authenticatorMakeCredential
- authenticatorGetAssertion
- authenticatorCancel

authenticatorMakeCredential 연산은 FIDO 1.0에서의 등록과 같이 RP에서 추후 인증에 사용할 수 있는 Credential을 생성한다. 이 연산은 호출자 Origin, RP Id, 계정정보, Attestation Challenge 등을 입력받아 Credential을 생성하고 저장한 후, 생성한 Credential과 이를 RP에서 확인할 수 있는 AttestationStatement를 함께 FIDO 클라이언트에게 반환한다.

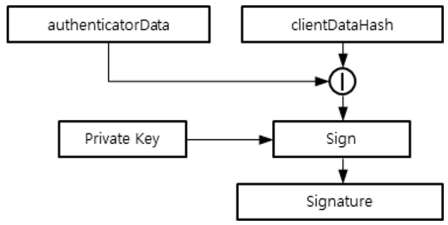
authenticatorGetAssertion 연산은 FIDO 1.0의 인증/서명과 같이 RP에게 인증장치에서 생성한 Credential을 이용하여 인증과 서명 기능을 제공한다. 이 연산은 호출자 Origin, RP Id, Assertion Challenge 등을 입력받아, 서명 값을 생성하고 해당 값을 FIDO 클라이언트에게 반환한다.

authenticatorCancel 연산은 FIDO 클라이언트에서 인증장치에게 요청한 위 두 연산을 취소하는 기능을 제공한다. 일반적으로 연산 처리가 TimeOut된 경우 등에서 이 연산이 호출되며 입력 인자와 반환 값은 없다.

4.2. FIDO 2.0 서명

FIDO 2.0 인증장치는 FIDO 클라이언트에서 전달하는 ClientDataHash와 인증장치 자체에서 생성하는 AuthenticatorData에 대해 개인키(Private Key)로 서명함으로써 서명 값을 생성한다. 이러한 공개키 서명 값은 인증장치가 Credential을 생성할 때 Attestation 용도로 사용되거나 인증장치가 생성한 Credential로 RP에게 인증/서명 기능을 제공할 때 사용된다[5].

AuthenticatorData는 사용자 로컬 인증을 수행하였는지 여부와 인증장치에서 수행한 서명 횟수를 나타내는 서명 카운터 정보로 구성된다. 선택적으로 확장 필드 정보를 포함할 수 있다. FIDO 2.0에서는 서명시 transaction 정보를 함께 서명할 수 있도록 하는 Transaction Authorization 확장 필드와 Credential 생성시 RP가 선호하는 인증장치를 제시할 수 있도록 하는 Authenticator Selection 확장 필드를 표준으로 정의하고 있다.



〔그림 3〕 인증장치 서명생성 절차

다음 그림은 인증장치에서 서명 값을 생성하는 것을 도식화한 것이다.

인증장치는 authenticatorData와 FIDO 클라이언트에서 전달받은 clientDataHash를 결합한 후 개인키로 공개키 암호화 연산을 수행하여 서명 값을 생성한 후, authenticatorData와 서명 값을 FIDO 클라이언트에게 반환한다.

4.3. FIDO 2.0 Attestation

FIDO 인증장치에서 Credential을 생성한 후, RP에게 전달하면 RP는 FIDO 인증장치에서 생성한 Credential의 신뢰여부를 확인할 수 있어야 한다. 이를 위해 FIDO 2.0에서는 다음 4가지 attestation 모델을 규정한다[6].

- Full Basic Attestation
- Surrogate Basic Attestation
- Privacy CA
- DAA(Direct Anonymous Attestation)

Full Basic Attestation 방식은 동일한 모델의 인증장치 그룹이 하나의 Attestation 키를 공유하도록 하여 인증장치 Attestation을 제공한다. Surrogate Basic Attestation은 인증장치에서 Credential을 생성한 후, Credential에 대응되는 개인키를 Attestation 용으로 사용하는 방식이다.

Private CA는 인증장치별로 Private CA와 안전하게 통신할 수 있는 키를 가지고 있어 다수의 attestation key 쌍을 생성하고 이에 대한 attestation 인증서 발급을 요청할 수 있다. 이 방식을 이용할 경우, FIDO

credential 각각에 대해 Attestation key를 발급받아 사용할 수 있게 된다.

DAA(Direct Anonymous Attestation) 방식에서는 인증장치가 단일 DAA 발급자에게 DAA credential들을 발급받아 attestation 데이터에 대한 blind 서명을 생성하는데 사용된다. 이를 통해 DAA Credential이 오용되는 것을 피할 수 있다.

4.4. 기타

FIDO Alliance에서는 FIDO 클라이언트가 설치된 사용자 단말에서 외부 인증장치와 통신하는 프로토콜을 표준화하는 문서 작업을 진행하고 있는 중이다.

이 문서는 인증장치에서 제공하는 연산과 각 연산에서 입력받고, 반환해야 하는 인자들을 정의하고 있으며 인증장치에 인자로 전달할 때 사용하는 메시지 인코딩 방식에 대하여 설명하고 있으며, 향후, USB, BLE 등과 같은 다양한 통신 수단과의 transport 바인딩, 에러 정의, W3C 웹 API와의 동기화 작업 등이 진행될 예정이다.

Ⅴ. 결 론

다양한 인증장치를 편리하게 사용할 수 있는 FIDO 범용인증기술은 현재 많은 업체들이 이미 개발하여 다양한 응용에 적용하여 사용하고 있다. FIDO 1.0이 주로 모바일 환경을 고려하여 설계되었다. 반면 FIDO 2.0은 다양한 요구사항을 수렴하여 웹 환경과 PC 환경에서도 FIDO를 사용할 수 있도록 플랫폼에서 지원하는 방향으로 설계되었다. 이를 통해 FIDO 2.0은 보다 폭넓은 응용서비스의 인증 및 전자서명 기술로 사용될 것으로 전망된다.

FIDO 1.0이 주로 서비스 제공자들이 주축이 되어 제공되었던 기술이라면 FIDO 2.0은 MS와 Google같은 플랫폼 업체들이 주축이 되어 기능이 제공될 예정이어서 미래에는 지금보다 더욱더 다양한 FIDO 기반의 인증장치들이 시장에 선보일 것으로 예상된다. 또한 FIDO 기술이 현재 주로 핀테크와 온라인 금융서비스 위주로 적용되고 있는 상황이나, 향후에는 IoT(Internet of Things)와 O2O(Online to Offline) 등 좀더 광범위한 분야의 인증/서명 기술로 사용될 것으로 전망된다.

결론적으로 국내 인증시장은 당분간 공인인증 기술의 대체 인증으로 FIDO 기술을 광범위하게 사용할 것으로 예상되며 FIDO의 확산에 따라 바이오 인증 기술도 더욱 더 발전할 것으로 예상된다.

참 고 문 헌

[1] Rob Philpott, Sampath Srinivas, John Kemp, UAF Architectural Overview. Version v1.0-rd-20140209, FIDO Alliance, February 2014.

[2] Sampath Srinivas, Dirk Balfanz, Eric Tiffany, Universal 2nd Factor(U2F) Overview. Versionv 1.0-rd-20140209, FIDOAlliance, February 2014.

[3] Rolf Lindemann, Davit Baghdasaryan, Eric Tiffany. FIDO Universal Authentication Framework Protocol. Version v1.0-rd-20140209, FIDO Alliance, February 2014. http://fidoalliance.org/specs/fido-uaf-protocol-v1.0-rd-20140209.pdf

[4] FIDO 2.0: Web API for accessing FIDO 2.0 credentials. URL: http://www.w3.org/Submission/2015/SUBM-fido-web-api-20151120/

[5] FIDO 2.0: Key attestation format. URL: http://www.w3.org/Submission/2015/SUBM-fido-key-attestation-20151120/

[6] FIDO 2.0: Signature format. URL: http://www.w3.org/Submission/2015/SUBM-fido-signature-format-20151120/

[7] 조상래, 최대선, 진승헌, 이형효, 패스워드 없는 인증기술 : FIDO, 전자통신동향분석 제29권, 제4호 통권 148호, 2014

〈저 자 소 개〉

조 상 래 (Sangrae Cho)
정회원

1996년 8월 : Imperial College London 전산학과 졸업
1997년 9월 : Royal Holloway, University of London 정보보안 석사
1997년 10월~1999년 7월 : LG종합기술원
1999년 7월~현재 : 한국전자통신연구원 인증기술연구실 책임연구원
<관심분야> 인증 및 인가 분야, 정보보호

조 영 섭 (YoungSeob Cho)
정회원

1993년 2월 : 인하대학교 전자계산공학과 졸업
1995년 2월 : 인하대학교 대학원 전자계산공학과 석사
1999년 2월 : 인하대학교 대학원 전자계산공학과 박사
1998년 12월~현재 : 한국전자통신연구원 인증기반연구실 책임연구원
<관심분야> 인증, ID 관리, 프라이버시 보호, 정보보호

김 수 형 (Soohyung Kim)
정회원

1996년 : 연세대학교 컴퓨터과학과 졸업(학사)
1998년 : 연세대학교 컴퓨터과학과 졸업(석사)
2016년 : 한국과학기술원 전산학과 졸업(박사)
1998년~2000년 : ㈜한국정보통신 기술연구소 연구원
2000년~현재 : 한국전자통신연구원 인증기술연구실 실장/책임연구원
<관심분야> 인증, 핀테크 보안, 개인정보보호, 모바일 지불결제