FIDO 기반 핀테크 인증 기술

김수형
한국전자통신연구원

요 약

최근 급격하게 확산되고 있는 핀테크 서비스는 다양한 분야의 사람들로부터 관심을 받고 있다. 기존 금융거래 프로세스에서 경험했던 불편함과 비효율을 개선하여 소비자와 기업 모두에게 편리성과 비용절감이라는 혜택을 제공하고, 새롭게 재편되고 있는 금융 산업에 참여할 기회를 제공하기 때문이다. 그러나 핀테크 서비스가 가져다 줄 혜택과 기회는 완벽한 보안에 기반하지 않으면 엄청난 피해를 야기할 수 있다는 우려도 존재한다. 본고에서는 핀테크 보안 기술 중 최근 급격히 관심을 받고 있는 FIDO (Fast IDentity Online) 인증 기술에 대해 살펴보고자 한다. 편의성과 보안성 측면에서 한계를 갖고 있던 기존 인증 기술들이 핀테크 서비스를 확산시키는데 장애가 되었다면, 최근 도입되기 시작한 FIDO 기술은 편리하고 강력한 인증을 제공하여 사용자와 기업 모두의 관심을 얻는데 성공하고 있는 것으로 보인다. 본 고에서는 FIDO 기술을 간단히 설명하고, FIDO 기술을 활용한 응용 보안 기술을 소개하고자 한다. 또한 FIDO 기술의 향후 발전 방향에 대해 현재 진행 중인 표준화 내용을 중심으로 살펴보고, 해외에서 활발히 진행되고 있는 연구들을 통해 핀테크 인증 기술의 발전 방향을 전망하고 결론을 맺는다.

Ⅰ. 서 론

금융 서비스에 IT기술이 접목되면서 발전해 온 핀테크 기술은 최근 국내뿐 아니라 전세계적인 관심을 받고 있는 분야이고 새로운 전자금융 시대를 열어갈 촉매제가 될 것으로 기대를 받고 있다. 오랜기간 동안 관련 기술과 서비스를 준비해온 해외와는 시기적인 격차가 존재하지만, 국내에서도 금융 업종에서 일어나고 있는 갑작스런 변화에 대응하고자 금융과 IT 기업들이 협력하여 새로운 금융환경에 적합한 서비스들을 발 빠르게 선보이고 있다. 예를 들어 최근 증가하고 있는 간편결제 서비스들과 생체인증기반 ATM 뱅킹 서비스들이 대표적인 사례들이다[1]. 현재까지 소개된 핀테크 서비스들의 핵심 가치는 불편한 거래수단 및 인증수단을 대체하여 사용자가 항상 소지하고 있는 스마트폰 또는 본인의 생체정보를 이용하여 간편하게 거래를 수행할 수 있는 방법을 제공하는데 있는 것으로 보인다. 그러나 편의성에 중점을 둔 핀테크 서비스의 급격한 증가는 대규모 금융보안 사고 발생에 대한 우려를 야기할 수 밖에 없다. 이러한 이유로 핀테크 보안에 대한 연구가 활발히 진행되고 있으며 핀테크 서비스들에 대한 보안성 분석[2][3][4]과 보안지침 표준 개발[5] 등의 작업들이 진행되고 있다.

핀테크 보안 기술은 거래수단의 간소화, 거래채널의 다양화, 본인인증의 편리성, 금융정보의 토큰화, 이상거래 탐지, 거래기기 보호 등 다양한 측면에서 원천 연구와 실용 기술 적용이 함께 이루어지고 있다. 신용카드 대신 스마트폰으로 거래하고, O2O/옴니채널을 통해 쇼핑하고, PIN과 QR코드로 본인인증하고, 신용카드대신 일회용 토큰정보로 결제 트랜잭션을 수행하고, 과거의 거래패턴과 사용자 프로파일을 통해 이상거래를 방지하고, 안전한 저장매체를 이용해 금융정보 및 인증정보를 보호하는 기술들이 현재 일반인들에게도 익숙한 핀테크 보안 기술에 해당된다. 그러나 이러한 기술들 각각은 자체적으로 해결해야 할 과제를 가지고 있으며 이에 따라 좀 더 다양한 연구가 필요한 상황이다. 본고에서 주로 다루게 될 본인인증 또한 마찬가지이다.

본인인증, 즉 사용자 인증은 우리의 삶에서 일상적으로 필요한 기술이다. 인터넷을 통해 쇼핑하고 스마트폰으로 SNS 활동과 스마트뱅킹 서비스를 이용하는 것에 우리는 이미 익숙해져 있다. 이러한 IT 기술에 기반한 사회생활에서 다양한 인터넷 서비스를 활용하기 위해서 사용자는 하나 이상의 ID를 등록하고 해당 ID가 사용자 본인의 것임을 증명할 수 있는 인증정보를 온라인 상에 등록하여야 한다. 활용 가능한 인증수단으로 현재까지 수 많은 인증기술들이 개발되고 소개되어 왔지만, 지식기반 인증수단의 범주에 속하는 '패스워드'를 대체할 만한 기술은 현존하지 않는다. 패스워드의 범용성과 편의성 그리고 비교적 저렴한 도입비용까지 고려한다면 앞으로도 상당 기간 패스워드는 보편적인 인증수단으로 활용될 것이라 예상할 수 있다. 그러나 '보안성'이라는 측면에서 패스워드 기술은 거의 한계에 도달한 것으

로 보인다. 사람이 가지는 기억력의 한계로 인해 보통 여러 사이트에서 동일한 패스워드를 사용함으로 발생하는 잠재적 위험들과 피싱사이트와 키로깅을 통해 쉽게 수집 당할 수 있고 유출된 패스워드를 누구나 사용할 수 있다는 정보의 속성으로 인해 패스워드는 비판의 대상이 되어 왔다. 패스워드의 보안 취약성을 보강하기 위해 OTP와 같은 2차 인증 기술을 도입하여 사용하는 것이 일반화되고 있어 더 이상 패스워드가 비용 효율적이고 편리한 인증 기술인지 판단하기도 쉽지 않다. 또한 최근의 핀테크 서비스에서는 패스워드의 보안 취약성이 금융거래 사고를 유발할 수 있다는 점에서 더욱 조심스러운 사용이 요구되고 있다.

위와 같은 패스워드 문제를 해소하기 위해서 등장한 기술이 본고에서 주로 다루게 될 FIDO (Fast IDentity Online) 기술이다. FIDO 기술 이전에도 패스워드를 대체하기 위한 다양한 인증 기술 연구가 진행되었지만, 〈그림 1〉과 같은 두 가지 해결하기 힘든 난관을 극복하지 못했다. 첫 번째로 지식기반 인증을 대체할 소유기반 인증 또는 생체기반 인증 기술을 적용한 경우에는 사용자 측에 하드웨어 장치와 해당 하드웨어를 제어할 소프트웨어 플러그인 모듈이 탑재되어야 하는 문제를 해결해야 한다. 그러나 국내의 공인인증서 이슈와 동일하게 소비자의 비용 발생과 이용 불편이라는 이슈는 해결되기 쉽지 않은 문제이다. 또한 서비스 기업의 입장에서는 해당 인증 기술을 도입할 때 관련 서버 모듈을 인증서버에 탑재해야 하는 이슈가 발생한다. 개별 인증 기술마다 서버모듈을 탑재해야 하기 때문에, 기술도입을 위한 많은 시간과 비용증가 문제 또한 해결하기 쉽지 않았던 것이다. 물론 한가지 인증기술이 패스워드만큼의 범용성을 보장해 준다면 소비자와 기업모두 투자할 가치가 있겠지만, 앞서 기술하였듯이 그러한 기술은 존재하지 않는다. 즉, 사이트마다 또는 기술마다 위와 동일한 문제를 겪을 수 밖에 없었다. 국내 기업들을 통해 최근에 개발된 다양한 인증기술 적용 시도도 동일한 문제를 가지고 기술 확산에 어려움을 겪고 있는 것이 사실이다.

그러나 IT 기술의 발전이 새로운 핀테크 시대를 열어가듯이

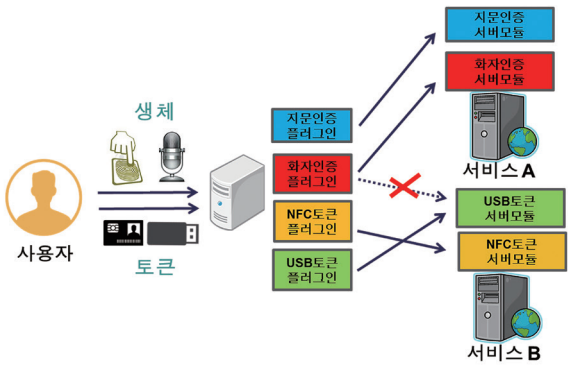

그림 1. 다양한 인증수단 적용 한계

인증기술 분야에서도 기존 문제들을 IT 기술의 도움으로 해결할 수 있는 실마리를 갖게 되었다. 스마트폰에 탑재되기 시작한 생체인식 센서의 증가, TrustZone 기술을 활용한 안전한 실행 영역의 확보, Trusted Computing 분야에서 오랫동안 연구되어온 신뢰보안 기술들, 그리고 지속적으로 발전되어온 Public Key Cryptography 등 암호 기술들이 결합되어 새로운 인증플랫폼인 FIDO 기술이 등장하게 된 것이다.

FIDO 기술에 대한 기술적인 내용은 이미 많은 자료에서 소개되고 있어[6][7], 본 고에서는 FIDO 기술을 간략하게 정리하고, FIDO 기술의 현황과 FIDO 기술을 활용한 응용보안 기술들을 중심으로 Ⅱ장에서 소개한다. 또한 FIDO 기술의 향후 발전 방향에 대해 현재 진행 중인 표준화 내용을 중심으로 살펴보고, 해외에서 활발히 진행되고 있는 연구들을 통해 핀테크 인증 기술의 발전 방향을 Ⅲ장에서 전망해 본다. 마지막으로 Ⅳ장에서는 본고의 내용을 정리하고 결론을 맺는다.

Ⅱ. FIDO 기술 현황 및 응용 기술 소개

FIDO 기술 표준[8]은 구글, 마이크로소프트, 비자, 페이팔, RSA, 인텔, 삼성 등 글로벌 업체가 참여하고 있는 FIDO Alliance에서 제정한다. FIDO 기술 표준을 통해 지식기반 인증, 소유기반 인증, 생체기반 인증 등 다양한 사용자 인증팩터를 지원할 수 있는 플랫폼을 구축할 수 있으며, 사용자에게는 안전하고 편리한 인증을, 서비스 기업에게는 중복투자 없는 표준기반 인증 서비스를 구축하는 장점을 제공한다.

FIDO 기술 표준은 크게 두 개의 표준으로 구분되는데, 첫번째는 UAF(Universal Authentication Framework) 표준으로 사용자의 스마트폰에 탑재된 인증수단(예: 지문인식 센서)을 온라인 서비스와 연동하여 사용자를 인증하는 기술이다. 두번째는 U2F(Universal 2nd Factor) 표준으로 기존 패스워드를 사용하는 온라인 서비스에서 2차 인증요소로 토큰기반 인증을 사용자 로그인 시에 추가할 수 있는 기술로 현재 크롬 브라우저를 통해 지원되고 있는 장점을 가지고 있다. 본 고에서는 패스워드를 대체하여 1차 인증요소를 지원할 수 있도록 하여 전세계적으로 관심을 받고 있는 기술인 FIDO UAF 표준을 중심으로 FIDO 기술을 설명한다.

FIDO UAF 아키텍처는 크게 사용자 기기와 사용자에게 서비스를 제공하는 웹 서버로 구성된다. 사용자 기기는 서비스를 제공하는 응용 앱(Relying-Party Application)과 사용자 인증을 수행하기 위한 FIDO 클라이언트로 구성되며, 웹 서버는 사용자에게 서비스를 제공하기 위한 응용 서버(Relying-Party

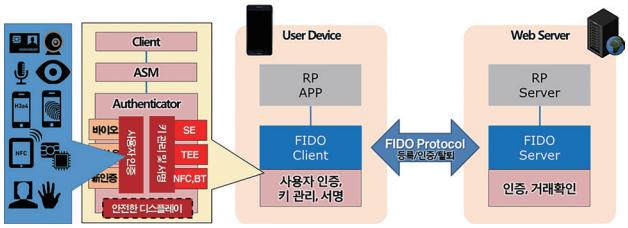

그림 2. FIDO UAF 아키텍처

Server)와 FIDO 서버로 구성된다. 〈그림 2〉는 FIDO UAF 아키텍처를 설명하기 위해, 표준에서 설명하는 내용을 기반하여 개략적으로 재구성한 것이다.

〈그림 2〉를 참조하여 FIDO UAF 아키텍처 및 각 구성요소의 역할을 좀 더 상세히 설명하면 다음과 같다. 사용자 스마트폰의 FIDO 클라이언트 모듈들의 구성은 FIDO 클라이언트, FIDO ASM (Authenticator Specific Module), FIDO 인증장치(Authenticator)로 구분된다. FIDO 클라이언트는 FIDO 서버와 FIDO 프로토콜을 수행하며 서비스 응용의 인증정책에 부합하는 인증장치가 사용되도록 지원하고, FIDO ASM은 FIDO 클라이언트가 FIDO 인증장치에 접근할 수 있도록 하며, FIDO 인증장치는 FIDO 프로토콜에서의 인증장치 등록/인증/탈퇴 및 실질적인 사용자 인증을 수행한다. FIDO 서버는 서비스 응용의 인증정책을 관리하여 해당 인증정책에 부합하는 FIDO 인증장치와 사용자 등록/인증/탈퇴에 필요한 프로토콜을 수행한다.

FIDO 기술은 기본적으로 사용자 스마트폰에 이미 탑재된 인증수단을 이용해 사용자를 로컬인증하고 인증된 사용자를 대신하여 사용자의 스마트폰(FIDO 인증장치)가 표준화된 단일 인증 프로토콜을 이용해 서버와 원격인증을 하는 구조를 채택하고 있다. 따라서 서비스 기업은 해당 서비스의 보안 요구수준에 적합한 다수의 인증수단들을 하나의 인증서버를 통해 사용자에게 제공할 수 있으며, 사용자는 본인의 스마트폰에서 익숙하게 사용하는 인증수단을 통해 서비스를 제공받을 수 있는 장점을 제공할 수 있는 것이다.

FIDO 기술은 프라이버시 측면에서도 장점을 갖고 있는데, 사용자의 민감한 생체정보가 사용자의 스마트폰에만 저장되어, 서버를 통해 생체정보가 유출될 수 있는 문제를 근본적으로 해결하고 있다. 또한 사용자를 특정할 수 있는 식별정보가 포함되지 않도록 FIDO 프로토콜이 설계되어 있어, FIDO 기술을 적용한 기업에서 대규모 DB 유출 사고가 발생하더라도 다른 사이트로 피해가 확산되는 것을 막을 수 있는 방안을 제시한다.

1. FIDO 기술 현황

FIDO 기술은 패스워드보다 편리하고 강력한 인증수단을 제공할 수 있다는 장점으로 전세계적인 관심을 받고 있는 표준 기술이다. 그러나 이러한 관심이 실제 서비스로 적용되어 확산하기 위해서는 크게 두 가지 해결과제를 갖고 있는 것으로 판단된다. 첫번째로는 관련 산업체에서 FIDO 기술을 신뢰할 수 있도록 하는 노력이 중요하다. 사용자 인증을 위한 플랫폼 기술로만 한정하여 보더라도 현재까지 많은 산업체 규격들이 개발되고 확산을 위한 노력들을 진행해 왔지만 일부 사이트에만 적용된 사례가 있어 대부분 몇 년이 지나 사람들의 기억에서 사라졌기 때문이다. 예를 들어 OpenID[9], CardSpace[10] 등은 기술 탄생 시점에 받았던 관심에 비해 현재 적용된 사이트는 확인하기 힘들 정도이다. 물론 OpenID는 지속적인 기술 발전을 모색하고는 있지만 아직 가시적인 성과가 확인되지는 않는다. 두번째로는 FIDO 제품의 신뢰성과 보안성을 확인하기 위한 절차와 지침을 준비하는 것이다. FIDO 기술 자체의 안전성과 프로토콜의 견고함은 전세계의 전문가들을 통해 몇 년간의 검증을 거치고 Global Platform, Trusted Computing 등 그룹에서 이미 채택되어 검증된 기술들을 활용해 개발된 것이긴 하지만, 실제 FIDO 기술 표준을 구현하는 세부적인 방법까지 구체적으로 명시한 것은 아니어서 구현 방식에 따라 보안성이 높은 제품과 낮은 제품이 상존할 수 밖에 없다. 따라서 FIDO 기술을 적용하려는 서비스 기업은 스스로 판단하여 신뢰할 수 있는 업체의 FIDO 제품을 사용하거나 업체가 직접 FIDO 기술을 개발하고 보안성을 검증하는 작업을 수행할 수 밖에 없다. 따라서 FIDO 기술의 빠른 확산을 위해서는 서비스 기업이 요구하는 수준의 신뢰성과 보안성을 제공하는 FIDO 제품 선택 기준과 방안이 마련될 필요가 있다.

일단 위에서 기술한 첫 번째 해결과제는 최근의 국내외 업체 동향을 살펴 볼 때 점차 긍정적인 방향으로 진행되고 있다고 판단된다. FIDO 기술이 제시하는 비전이 매력적인 측면도 있겠지만, 급격히 증가하는 230여개 이상의 글로벌 멤버들과 현재의 기술 규격에 머무르지 않고 새로운 플랫폼으로 확장 발전을 위한 노력들이 객관적인 평가를 가능하게 한다. 또한 FIDO 기술 규격이 제시하는 생태계는 특정 몇 업체의 이익을 보장해주는 형태가 아니라 참여하는 모든 업체들이 시장을 개척해 나갈 수 있는 기회를 제공하는 것이라 더 긍정적인 평가가 가능해진다. FIDO 기술 정식 표준을 처음 발표한 시기는 2014년 12월이지만, 페이팔-삼성, 알리바바, ETRI-BC카드 등이 발표 이전에 파일럿 서비스를 진행한 바 있으며, 2015년 5월 이후에 삼성페이, NTT DOCOMO, BOA(Bank of America)에서 FIDO UAF 기술의 상용서비스를 런칭하였다. 또한 Google, DropBox, GitHub 등은 FIDO U2F 기술의 상용서비스를 제공하고 있다. 최근 국내에서는 BC카드, 하나금융, NH농협 등이 FIDO 기술을 이용한 상용서비스를 런칭할 예정이라고 발표한 바도 있다.

FIDO 제품의 신뢰성과 보안성 문제는 여러 측면에서 다루어지고 있는데, 현재 FIDO 연합에서는 자체적으로 FIDO Certification 프로그램을 준비하여 특정업체의 FIDO 제품이 FIDO 표준 규격에 적합한지, 타사의 FIDO 제품들과 상호연동이 잘 되는지를 검증하는 시험을 실시하고 있다. 따라서 FIDO Certified 제품의 경우에는 기능적인 측면에서의 신뢰성은 보장된다고 할 수 있다. 하지만 보안성에 대해서는 FIDO 연합에서 검증하는 절차를 실시하지 않는다. FIDO 인증장치에서 제공하는 사용자 인증수단들은 무수히 많은 방식과 알고리즘들을 통해 구현될 수 있기 때문에, 하나의 검증절차로 모든 제품의 보안성을 확인할 수 있는 방안은 존재하지 않는다. 따라서 FIDO 인증장치의 보안성은 사용자 인증수단과 FIDO 표준규격에서 정의하고 있는 인증정보의 관리 및 사용을 분리해서 평가할 필요가 있다. 즉, 인증정보가 안전한 실행영역에서 확인되고 이용되는지, FIDO 프로토콜에 사용되는 암호화 및 전자서명 키는 안전하게 저장되고 관리되는지 등을 평가할 수 있는 지침을 만드는 것을 선행할 필요가 있다. 다만 FIDO 인증수단의 안전성(예를 들어, 생체기반 인증장치의 EER 등)을 평가하는 방안은 좀 더 많은 준비가 요구되고 있다.

FIDO 기술의 보안성은 사용자 인증을 실질적으로 수행하는 FIDO 인증장치의 보안성에 크게 영향을 받는다. 즉, FIDO 인증장치에 적용된 인증 기술 및 보안 기술에 따라 FIDO 기술을 채택한 서비스의 보안성이 좌우되기 때문이다. 따라서 이용 편의성뿐만 아니라 보안성이 중요한 핀테크 서비스에서는 FIDO 기술의 채택에 있어서 다음과 같은 항목을 고려해야 한다.

(1) 사용자 인증: FIDO 기술은 생체기반 인증을 비롯해 소지기반 인증, 지식기반 인증 기술을 모두 지원할 수 있도록 설계되어 있다. 따라서 서비스의 보안 요구수준에 맞는 인증 기술을 선택하여 제공하는 것이 필요하다. 예를 들어, 높은 수준의 보안이 필요한 서비스는 스마트카드와 같은 HW토큰을 활용하는 것도 고려해 볼 수 있다. 또한 두 가지 이상의 인증 기술을 결합해서 제공하는 것도 가능하다.

(2) 안전한 저장: FIDO 인증장치에 저장되는 정보 중, 인증정보, 전자서명 생성키 등은 H/W 보호 메커니즘을 활용하는 것을 권장하고 있다. 현재 상용화된 FIDO 인증장치는 대부분 TrustZone 기술을 활용해 인증정보와 전자서명 생성키를 보호하고 있지만, USIM 또는 스마트폰과 연결된 외부기기(예: 스마트워치와 같은 블루투스 기기 등)에서 해당 정보를 안전하게 관리하고 이용하는 것도 고려해 볼 수 있다.

2. FIDO 기술의 활용

FIDO UAF 기술은 2016년 1월 현재 국내에서는 안드로이드 스마트폰의 생체인증 장치를 통해서만 서비스에 활용되는 중이다(예: 삼성페이의 지문인증 결제). 하지만 아이폰의 터치아이디 기술을 연계한 FIDO 기술과, 스마트카드, 스마트와치 등을 인증장치로 활용하는 기술이 ETRI에서 개발 완료되어 다양한 스마트 기기에서 FIDO 기술을 조만간 활용할 수 있으리라 기대되고 있다. 스마트카드 인증장치는 FIDO 보안 모듈이 탑재된 스마트 카드를 스마트폰에 터치(NFC: 근거리무선통신)하여, FIDO 인증에 필요한 전자서명 및 암호화를 스마트폰 대신 스마트 카드 내에서 수행하는 방식으로 구현된 것으로 암호화에 필요한 보안 정보는 사용자의 스마트카드에만 저장되어 유출 위험에 안전하다는 장점을 갖는다. 높은 보안성이 요구되지만 스마트폰의 Trust Zone 기술 또는 Secure Element (예: USIM) 기술을 활용할 수 없는 서비스에서 고려될 수 있다.

FIDO 기술은 현재 PC/브라우저를 대상으로는 활용되지 않고 있다. III장에서 소개되는 FIDO 2.0 기술이 국제표준으로 채택되면 향후 PC/브라우저에서도 지원될 예정이지만 국제표준 채택과 PC, 노트북 등에 FIDO 기반 생체인식 센서를 탑재하는 것은 단기간에 이루어지기 쉽지 않다. 따라서 스마트폰에 적용된 FIDO 기술을 PC/브라우저에서도 활용할 수 있도록 하는 연구가 진행되고 있다. 대표적으로 전세계 이동통신사업자협회인 GSMA의 Mobile Connect 기술[11]과 FIDO 기술을 결합한 기술이 그것이다. Mobile Connect 기술은 사용자가 소지한 스마트폰을 인증 수단으로 활용하기 위한 것으로 SMS 휴대폰 인증의 발전된 형태라고 할 수 있다. Mobile Connect 기술과 FIDO 기술을 결합하면 소지기반 인증과 생체기반 인증을 함께 제공할 수 있어 SMS 인증보다 강력한 인증이 가능하다. 〈그림 3〉은 GSMA에서 제안한 것으로 FIDO 기술을 통해 이동통신업체가 FIDO 기반 생체인증을 수행하고, 서비스 기업은 이동통신업체로부터 SAML, OpenID와 같은 ID Federation 기술을 통해 사용자의 본인여부 또는 사용자의 속성정보를 제공받을 수 있는 방안을 제시하고 있다. 즉, PC/브라우저에서 요청된 서비스를 제공하기 위해서 사용자 본인여부와 속성정보를 이통사를 통해

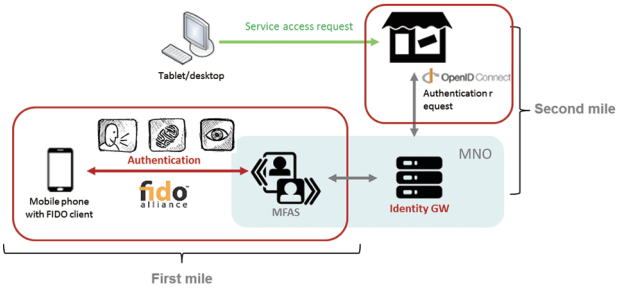

그림 3. Mobile Connect와 FIDO

제공 받는 서비스로, 국내 통신3사에서도 관련 준비를 진행하고 있는 것으로 확인되고 있다.

FIDO 기술을 PC/브라우저에서 활용하는 기술은 〈그림 4〉와 같은 절차를 통해 일반적으로 수행된다. 휴대폰을 인증수단으로 이용하는 기술은 오래 전부터 연구되어온 것[12]으로 새로운 기술은 아니지만 최근의 기술은 이전의 절차를 좀 더 편하면서 안전하게 수행할 수 있는 방법을 제시한다. 〈그림 4〉의 인증 절차를 세부 단계별로 설명하면, ① 사용자가 인증을 요청하는 단계 ② 서비스 서버가 사용자의 스마트폰에 푸시서비스를 통해 인증 요청을 전달하는 단계 ③ 스마트폰의 인증 앱이 자동 실행되어 서비스 서버를 통해 FIDO 인증 프로토콜을 요청하는 단계 ④ 사용자가 스마트폰에 탑재된 인증장치를 통해 인증하는 단계 ⑤ FIDO 인증 프로토콜을 수행하는 단계 ⑥ 서비스 서버가 인증결과를 확인 후에 서비스를 제공 단계로 구성된다. 사용자 측면에서는 매우 단순한 절차로 인증을 수행할 수 있다. 예를 들어, 사용자는 브라우저에서 마우스를 한번 클릭하고 스마트폰을 들고 지문을 터치하는 것으로 본인인증을 수행할 수도 있다.

그림 4. 스마트폰을 활용한 PC 로그인/인증

FIDO 기술은 온라인 인증에서뿐만 아니라 오프라인 환경에서의 접근통제 서비스에도 활용될 수 있다. 〈그림 5〉는 FIDO 기술을 활용한 출입통제 시나리오이다. 사용자 출입을 위한 절차를 세부 단계별로 설명하면, ① 출입통제 장치에서 주기적으로 비콘 메시지를 전송하고 사용자가 해당 출입통제 장치에 근접한 경우에 비콘 메시지를 수신하여 출입통제에 필요한 인증절차를 준비하는 단계 ② 사용자가 소지한 스마트폰 또는 스마트워치를 통해 FIDO 인증 프로토콜을 수행하는 단계 ③ FIDO 인증 프로토콜을 완료 후에 출입통제에 필요한 인증토큰을 발급 받는 단계 ④ 인증토큰을 출입통제 장치에 전달하고 출입통제 장치는 전달된 인증토큰을 확인하여 출입여부를 결정하는 단계로 구성될 수 있다.

〈그림 5〉의 ① 단계 비콘 메시지는 BLE (Bluetooth Low Energy) 기기를 통해 생성할 수 있으며, ② 단계에서 필요한 사용자 인증은 출입통제에 요구되는 보안 수준에 따라 생체기반 인증, 소유기반 인증 등을 수행할 수 있고, ④ 단계에서 인증토큰을 전송하는 방법은 BLE 또는 NFC HCE (Host-based Card Emulation) 통신 기술을 사용할 수 있다.

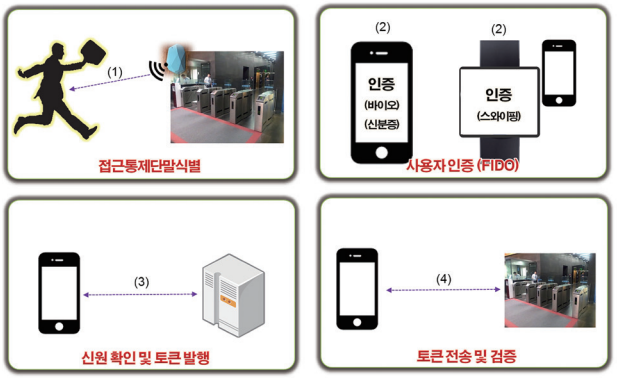

그림 5. FIDO 기술을 활용한 출입통제 시나리오

위의 출입통제 시나리오에서 설명된 기술은 강력한 본인확인이 요구되는 다양한 O2O (Online to Offline) 서비스에도 동일하게 적용될 수 있다. FIDO 기술은 위와 같이 기존의 온라인기반 핀테크 서비스 외에도 사용자 인증이 요구되는 다양한 환경의 서비스에 응용되어 사용될 수 있다.

Ⅲ. FIDO 2.0 기술과 멀티팩터 인증

1. FIDO 2.0 기술의 등장

FIDO 기술은 계속적으로 진화하고 있는 기술이다. 현재 서비스 중인 FIDO 1.0 기술은 스마트폰이라는 제한된 플랫폼에서만 제공되고 있지만, 향후에는 웹브라우저를 통해 플랫폼 제약 없이 사용될 수 있을 것으로 예상되고 있다. PC/웹브라우저까지 FIDO 기술을 확장한 FIDO 2.0 규격이 거의 완성단계로 준비되고 있기 때문이다. FIDO 기술은 이름(Fast IDentity Online)에서도 알 수 있듯이 온라인 사용자 인증을 간편하게 제공하기 위한 기술이다. 대부분의 사용자 인증이 웹브라우저를 통해 수행되는 현재의 인터넷 환경에서는 스마트폰을 대상으로 하는 FIDO 1.0 기술의 확장은 필수적이다. FIDO 연합은 이를 위해서 스마트폰 중심의 FIDO UAF 규격과 크롬 웹브라우저에서 지원하고 있는 FIDO U2F 규격을 통합한 FIDO 2.0 규격을 준비하고 있으며, 해당 규격의 초안을 W3C (World Wide Web Consortium) 표준화 기구에 제출하여 국제표준으로 채택시키기 위한 노력들을 진행 중이다. 해당 규격이 W3C 표준으로 채택되면, 〈그림 6〉과 같이 웹브라우저가 FIDO 클라이언트 역할을 수행하여 사용자 기기에 설치된 FIDO 인증장치와 연계한 다양한 인증 기술들을 사용자에게 제공할 수 있게 된다. 예를 들어, 지

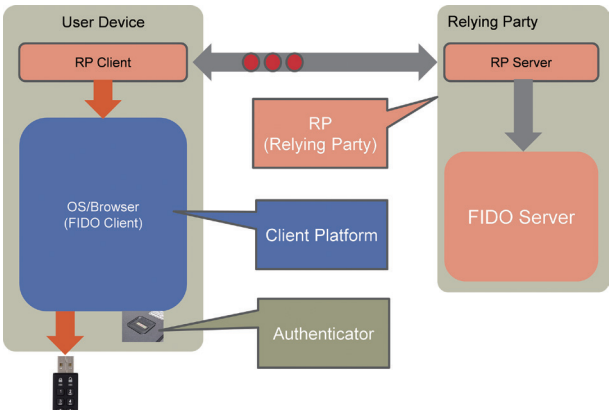

그림 6. FIDO 2.0 아키텍처 (출처: FIDO 협회)

문인식 모듈이 탑재된 노트북에서는 지문인증으로 온라인 뱅킹 사이트에 로그인하고, 홍채인식 모듈이 탑재된 태블릿에서는 인터넷 쇼핑 결제를 홍채인증으로 간편히 수행할 수 있는 것이다.

FIDO 2.0 기술 규격은 구글과 마이크로소프트를 중심으로 진행되고 있어, FIDO 2.0 기술의 웹브라우저 적용은 일반적인 W3C 표준적용보다 빠르게 진행될 수 있을 것으로 예상된다. 그리고 FIDO 아키텍처의 중간자 역할을 수행하는 FIDO 클라이언트를 OS 및 브라우저 제조사들이 제공하여 FIDO 기술의 신뢰성을 더 높이는 계기가 될 수 있으며, 인증기술 솔루션 기업과 핀테크 서비스 기업들은 인증장치 또는 인증서버만 고려하여 사업을 진행할 수 있어 FIDO 기술 확산에 장점을 얻을 수 있다. 또한 OS 및 브라우저 제조사들은 사용자가 이용하고자 하는 서비스의 일차 관문인 인증플랫폼을 확보할 수 있어 자사의 플랫폼을 좀 더 확장할 수 있는 기회를 얻게 된다. 물론 기존의 생체인식 센서 및 보안 모듈을 제공하는 기업에서도 PC 영역까지 사업을 확장할 수 있는 기회를 얻을 수 있다.

사용자 입장에서도 FIDO 2.0 기술을 통해 혜택을 받을 수 있다. 사용자 본인의 노트북/PC 또는 웹 환경에서도 생체기반 인증, 소지기반 인증을 사용할 수 있게 되어 더 이상 패스워드를 기억해야 하는 불편함과 보안에 대한 불안을 겪지 않아도 되는 것이다. 아직까지 일부 노트북/PC에서만 생체인식 센서를 탑재하고 있어서 FIDO 2.0 기술을 사용하기까지 좀 더 많은 시간이 필요할 수 있다. 그러나 FIDO 2.0 기술은 생체인식 센서 탑재가 일반화되고 있는 스마트폰을 노트북/PC의 외부 인증장치로서 활용하는 기술 규격도 함께 개발하고 있어, 이러한 문제를 어느 정도 해소할 수 있을 것이다. 예를 들어, 노트북을 통해 웹 쇼핑을 할 때, 사용자가 소지한 스마트폰에 지문을 대고 결제하는 시나리오도 가능하게 된다. 이전 FIDO 1.0에서 푸쉬서비스를 통해 스마트폰과 웹 서버간 연계하여 서비스하는 방식은 사전에 사용자 스마트폰 정보를 서버에 등록하는 과정을 거쳐야 하지만, FIDO 2.0에서는 등록 과정 없이 웹브라우저와 사용자의 스마트폰이 블루투스와 같은 근거리 통신기술을 통해 직접 연결되어 복잡한 절차 없이 서비스가 가능해진다.

2. 멀티팩터 인증 기술

FIDO 기술을 통해 도입되기 시작한 생체인증 기술은 패스워드 기술 중심의 핀테크 서비스에 커다란 변화를 가져다 주고 있다. 기존의 서비스에서 느끼지 못했던 편리함을 생체인증이라는 기술을 통해 경험하고 있기 때문이다. 편리한 인증 기술에 한번 익숙해진 사용자들에게 다시 패스워드를 입력하라고 요구하는 것은 어려운 작업일 것이다. 이러한 변화의 시기에 핀테크 서비스의 보안을 담당하는 책임자와 연구자들은 좀 더 많은 고민을 할 수밖에 없다. 안전하게 관리한다는 가정 하에서 사용되는 패스워드는 아직까지 유효한 인증수단이기 때문에 패스워드를 대체하여 적용한 새로운 인증수단은 최소 패스워드 이상의 편의성을 제공하든지 또는 패스워드 이상의 안전성을 제공할 수 있어야 한다. 이러한 측면에서 생체인증 기술은 보안성을 객관적으로 증명할 수 있는 연구, 즉 인식률을 개선하기 위한 연구외에도 보안성 평가 방법론에 대한 준비가 지속적으로 수행될 필요가 있다. 그리고 보안성을 보강하기 위해서 다양한 인증수단을 결합한 멀티팩터 인증의 도입을 고려할 수도 있다. 최근의 연구 동향을 살펴보면, 멀티팩터 인증은 새로운 인증 환경에 적합한 최선의 선택이 될 수 있을 것으로 보여진다[13][14][15]. 사용자가 원하는 방식으로 또는 사용자 기기가 지원할 수 있는 방식으로 인증수단을 제공하기 위해서는 다양한 인증수단을 유연하게 결합할 수 있는 방안이 준비되어야 한다. 멀티팩터 인증을 제공하기 위해서 선택할 수 있는 인증수단은 여러 가지가 있을 수 있겠지만, 사용자의 불편을 고려한다면, 최소한의 명시적 인증(예를 들어, 지문인증)과 다양한 무자각 인증 기술을 결합하는 것이 요구될 수 있다. 최근에 활발히 진행되는 연구 주제들은 이러한 무자각 인증 기술로서 활용될 수 있다[14][15]. 예를 들어, 키보드 타이핑, 화면 터치 등의 행위 패턴을 지속적으로 분석하는 기술과 이용 기기나 주변 기기가 생성하는 고유한 정보(디바이스 핑거프린트, WiFi/블루투스 시그널 등)를 이용한 상황인지 기반 인증 기술도 중요한 연구 주제이다. 이러한 기술은 기존의 이상거래탐지 시스템(FDS, Fraud Detection System)과 유사하지만 사용자 이용기기에서 획득할 수 있는 다양한 정보들을 기반으로 더 정밀하게 사용자 본인여부를 지속적으로 파악할 수 있는 핀테크 서비스 환경을 제공할 수 있다. 따라서 사용자는 자신이 명시적으로 수행하는 인증수단보다 높은 수준의 보안을 보장 받으면서도 불편 없이 서비스를 이용할

수 있게 된다.

Ⅳ. 결 론

본고에서는 FIDO 기술을 중심으로 핀테크 인증 기술의 현재와 미래에 대해 살펴보았다. FIDO 기술은 개별적인 인증수단이 아닌 다양한 인증수단을 수용할 수 있는 플랫폼으로서 현재까지 연구된 어떠한 인증기술들보다 강력한 흐름을 만들어 내고 있다. 이는 기술자체의 우수성이 역할을 한 것일테지만, 생체인식 센서, TrustZone 등 최신의 보안 기술을 탑재한 스마트폰의 발전과 강력한 인증을 필요로 하는 핀테크 서비스의 확산이 뒷받침하고 있는 것도 크게 영향을 미쳤으리라 판단된다. FIDO 기술은 보다 다양한 기기, OS, 브라우저를 지원하며 사용자 인증을 위한 기본적인 플랫폼으로 자리잡으리라 예상되며, 보다 다양한 응용 분야에서 활용될 것으로 기대된다. 그러나 이를 위해서는 산업체의 이해를 돕기 위한 폭넓은 활동과 도입에 필요한 절차, 지침, 기준 등을 준비하는 노력도 필요하다. 또한 단일 팩터 인증 기술이 갖는 한계를 극복하기 위해 다양한 인증기술들을 수용하고 사용자의 이용 불편 없이 제공해 줄 수 있는 새로운 인증기술의 연구가 요구된다.

Acknowledgement

본 연구는 미래창조과학부 및 정보통신기술진흥센터의 정보통신·방송 연구개발 사업의 일환으로 수행하였음 [B0126-15-1007, "상황인지 기반 멀티팩터 인증 및 전자서명을 제공하는 범용 인증 플랫폼 기술 개발"].

참 고 문 헌

[1] 금융보안원 보안연구부 보안기술팀, "생체정보를 이용한 금융 서비스 현황 비교 분석,"2015.12.

[2] 허세경, "핀테크 관련 보안기술 분석," 전자금융과 금융보안 창간호, 2015.7. 101-113.

[3] 금융보안원 보안연구부 기술기술팀, "주요 간편 결제 서비스의 보안성 비교 분석," 전자금융과 금융보안 제2호, 2015.10.

[4] 박정국, "정보보안 관점에서 핀테크 서비스에 대한 이해와 대응," 지급결제와 정보기술 제 61호, 2015.7.

[5] 김신영, "전자금융거래의 사용자 인증방법 평가 및 선택 가이드," 전자금융과 금융보안 제2호, 2015.10, 59-94.

[6] 김수형, 조영섭, 최대선, " 핀테크 시대: 새로운 인증 기술을 요구하다," 정보과학회지 제33권 제5호, 2015.5, 17-22.

[7] 김수형, 진승헌, "FIDO 유니버셜 인증 프레임워크 (UAF) 제1부 ~ 제11부,"한국정보통신기술협회 표준문서, 2015.12.

[8] FIDO Alliance, "UAF & U2F Specifications," 2014.12. https://fidoalliance.org

[9] OpenID Foundation, "OpenID," http://openid.net/

[10] Microsoft, "CardSpace," https://msdn.microsoft.com/en-us/library/aa480189.aspx

[11] GSMA, "Mobile Connect," http://www.gsma.com/personaldata/mobile-connect

[12] SooHyung Kim et al., "Context-Aware Service System Architecture based on Identity Interchange Layer," in 2008 10th International Conference on Advanced Communication Technology, 2008, vol. 2, pp. 1482-1486.

[13] Weizhi Meng et al. "Surveying the Development of Biometric User Authentication on Mobile Phones," IEEE Communications Surveys & Tutorials, VOL 17, NO 3, 2015, 1268-1293

[14] Nikolaos Karapanos et al. "Sound-Proof: Usable Two-Factor Authentication Based on Ambient Sound,"USENIX Security, 2015, 483-498.

[15] Nan Zheng et al. "You Are How You Touch: User Verification on Smartphones via Tapping Behaviors," 2014 IEEE 22nd International Conference on Network Protocols (ICNP), 2014, 221-232

약 력

김 수 형

1996년 연세대학교 공학사
1998년 연세대학교 공학석사
2016년 한국과학기술원 공학박사
1998년~2000년 한국정보통신 연구소 연구원
2000년~현재 한국전자통신연구원 인증기술연구실 실장 / 책임연구원
관심분야: 핀테크보안, 사용자인증, 개인정보보호, 모바일보안, IoT보안 등