ETRI

2018
Electronics and
Telecommunications
Trends

블록체인 기반의 FIDO 범용 인증 시스템

FIDO Universal Authentication System Based on Blockchain

김석현 (S.H. Kim, ksh4uu@etri.re.kr) 정보보호연구본부 선임연구원
허세영 (S.Y. Huh, one@etri.re.kr) 정보보호연구본부 연구원
조영섭 (Y.S. Cho, yscho@etri.re.kr) 정보보호연구본부 책임연구원
조상래 (S.R. Cho, sangrae@etri.re.kr) 정보보호연구본부 책임연구원/PL
김수형 (S.H. Kim, lifewsky@etri.re.kr) 정보보호연구본부 책임연구원/기술총괄 PL

In this paper, we describe a FIDO universal authentication system based on a Blockchain that can share the user's FIDO authentication information between the application services of multiple domains without the use of a server. In addition we provide a method to query the FIDO authentication information of the user recorded in the Blockchain using only the user's service ID. Therefore, even if the user executes the FIDO registration process only once, the user can use the FIDO authentication service of another application service without repeating an additional FIDO registration procedure, and the service provider can securely share and utilize the FIDO authentication information of the user without the use of a trusted third party, thereby lowering the deployment and maintenance costs of the FIDO server.

* DOI: 10.22648/ETRI.2018.J.330104

*이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원[No. 2015-0-00168, 상황인지기반 멀티팩터 인증 및 전자서명을 제공하는 범용인증플랫폼기술 개발]과 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임[No.2016-0-00097, 비대면 본인확인을 위한 바이오 공개키 기반 구조 기술 개발].

4차 산업혁명 사회의 초연결 지능과 신뢰 인터넷 기술 특집

Ⅰ. 서론

인터넷 서비스를 이용하기 위해서는 사용자 등록과 사용자 인증 과정은 필수적이다. 하지만 모든 서비스에 동일한 개인정보를 반복적으로 입력하고 서로 다른 인증 정보를 설정하여 이용하기에는 많은 불편이 따른다. 이러한 불편 때문에 최근 '소셜 로그인' 서비스가 대중화되고 있다[1]. 2016년에 조사한 자료에 따르면 93%가 소셜 로그인을 선호하고, 소셜 로그인을 사용하는 가장 큰 이유가 회원 가입 및 등록 절차의 번거로움과 별도의 아이디 및 패스워드 생성 및 관리의 번거로움 때문이라고 한다[2]. 하지만 일각에서는 소셜 로그인 서비스의 아이디와 패스워드가 해킹당할 경우, 해당 서비스뿐만 아니라 다른 응용 서비스의 개인정보까지 쉽게 해킹당할 수 있는 심각한 보안 문제가 발생할 수 있다고 경고한다[3].

최근 모바일 단말에 지문과 홍채, 얼굴과 같은 생체인식 기술이 탑재되면서 사용자의 생체정보를 활용하여 사용자를 인증할 수 있는 FIDO(Fast Identity Online) 기술이 확산되고 있다[4]. FIDO 인증 기술은 온라인 환경에서 패스워드 대신 생체 정보를 활용하여 빠르고 안전하게 사용자를 인증할 수 있는 범용 인증 플랫폼이다. FIDO 인증 시스템은 공개키 기반 구조의 인증 기법을 사용하기 때문에 사용자 인증을 위한 공개키를 서버에 등록하는 과정이 필요하다. 향후 FIDO 인증 시스템을 도입한 서비스가 증가할수록 사용자는 반복적인 FIDO 등록 과정을 요구받게 될 것이고, 이러한 반복적인 등록 과정의 번거로움을 해소하고 사용자의 편의성을 향상시키기 위해서 소셜 로그인과 같은 방식의 FIDO 인증 서비스가 제공될 수 있다.

본고에서는 서버 없이 여러 도메인의 응용 서비스 간에 사용자의 FIDO 인증 정보를 안전하게 공유하고 이용할 수 있는 블록체인 기반의 FIDO 범용 인증 시스템을 기술한다. 특히 블록체인 기반의 FIDO 인증 정보를 모든 응용 서비스가 조회할 수 있는 방안으로 사용자의 서비스 ID만을 이용하여 처리할 수 있는 방법을 제시한다. 이를 통해서 사용자는 FIDO 등록을 한 번만 수행하고 추가적인 FIDO 등록 절차와 인증 정보 제공 없이 모든 사이트의 FIDO 인증 서비스를 이용할 수 있으며, 서비스 제공자는 공인된 제3의 기관을 이용하지 않고 사용자의 FIDO 인증 정보를 안전하게 공유하고 활용하여 FIDO 인증 서비스를 제공할 수 있다.

본고의 구성은 다음과 같다. Ⅱ장에서 FIDO 기술과 블록체인 기술에 대하여 기술하고, Ⅲ장에서 블록체인 기반의 FIDO 범용 인증 시스템의 구조 및 설계에 대하여 기술한다. Ⅳ장에서는 블록체인 기반의 FIDO 범용 인증 시스템을 이용한 FIDO 등록, 인증, 블록체인 ID 조회 기능을 설명하고, Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 기술

1. FIDO 인증 기술

FIDO연합은 2013년 2월에 정식 출범하여, 2014년 12월 생체 정보를 활용한 범용 인증 프레임워크인 FIDO 1.0을 발표하였다[5]. 2015년 11월 웹 브라우저에서도 사용할 수 있도록 FIDO 2.0 웹 API 표준 초안을 W3C에 제출하였고, 2018년 상반기에 표준이 완료될 것으로 예상된다[6], [7].

FIDO 인증 기술의 기본 철학은 사용자 단말에 적용되어 있는 다양한 인증 수단을 온라인 서비스의 사용자 인

(그림 1) FIDO 인증 기술

증 수단으로 사용할 수 있도록 하기 위함이고, 이를 위해서 사용자 확인(User verification), 인증 프로토콜(Authentication protocol) 및 인증 서버를 (그림 1)과 같이 분리하였다. 이러한 구조적 특성은 사용자 측면에서 다양한 인증 수단을 사용할 수 있고, 사업자 측면에서는 한 번에 투자로 다양한 사용자의 인증 수단을 수용할 수 있는 장점이 있다. 그리고 사용자 확인은 해당 디바이스 내부에서만 동작하므로 사용자의 지문과 같은 생체 정보가 FIDO 인증 서버로 전송되지 않아 생체 정보 유출로 인한 프라이버시 문제에서도 자유롭다[8].

FIDO 인증 시스템의 동작을 간략하게 설명하면, 첫 번째로 사용자 확인 단계이다. 사용자 확인 단계는 FIDO 인증 장치가 지원하는 인증 수단을 이용하여 사용자가 해당 인증 장치에 등록되어 있는 사용자인지 확인하는 과정이다. 예를 들면, 스마트 단말의 지문인식 기능을 통해서 사용자를 인증하는 방법과 같다. 두 번째로 FIDO 인증 장치와 서버 간에 인증 단계이다. 인증을 위해서 공개키 기반 구조의 인증 기법을 사용한다. 공개키 기반의 인증 기법을 사용하기 위해서는 서명을 위한 개인키와 검증을 위한 공개키가 필요하며, 이 키 쌍들은 FIDO 인증 장치에서 사용자 확인 과정이 정상적으로 완료되었을 경우에만 자체적으로 생성하고 관리한다. 그리고 FIDO 인증 장치는 생성된 공개키를 FIDO 서버에 등록하고, 이후 사용자 인증이 필요한 경우에 FIDO 인증 장치가 개인키로 서명한 인증 정보를 FIDO 서버에 등록되어 있는 공개키로 검증하는 방식이다. 따라서 사용자가 FIDO 인증 서비스를 이용하기 위해서는 최초 한 번의 FIDO 등록 과정이 필요하다.

2. 블록체인 기술

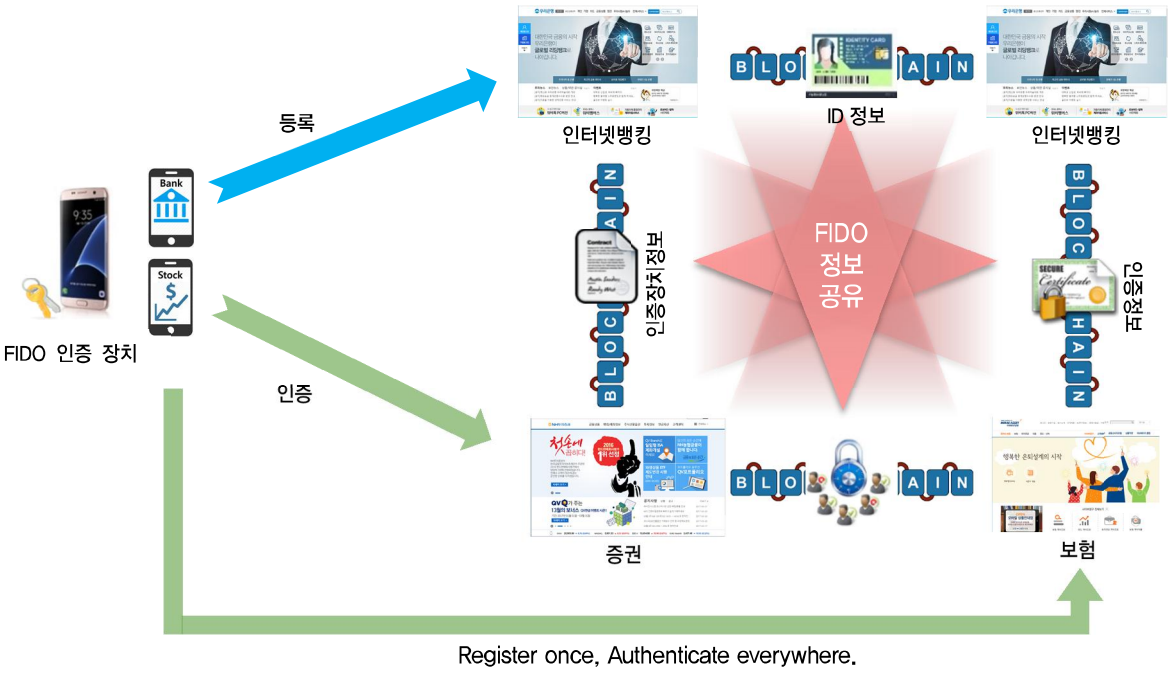
블록체인 기술은 네트워크 내 모든 참여자가 거래 정보를 공유·검증·기록할 수 있는 기술[9]이며, 거래 정보가 기록되는 거래 장부는 네트워크에 참여하는 모든 참여자에게 분산 저장되기 때문에 참여자가 모두 해킹되지 않는 이상 조작이 불가능하다. 또한, 공유되는 거래 정보의 유형도 일반적인 데이터 형식과 특정한 기능을 수행하도록 프로그래밍이 된 스마트 컨트랙트(Smart contract)이 있다. 스마트 컨트랙트는 블록체인 네트워크 참여자가 동시에 동일한 코드를 실행하고 결과를 검증하여 모두 동일한 경우에만 그 결과를 블록체인의 거래 장부에 기록하거나 수정할 수 있도록 설계할 수 있는 프로그램이다. 따라서 공인된 제3의 기관을 이용하지 않아도 블록체인 네트워크에 참여하는 모든 참여자가 스마트 컨트랙트를 통해서 기록되는 정보를 신뢰할 수 있다.

이러한 블록체인의 공유 기술을 통해서 서로 다른 도메인 간에 FIDO 인증 정보를 공유할 수 있다면, 사용자는 반복되는 FIDO 등록 절차를 단 한 번으로 줄일 수 있고, 서비스 제공자는 공인된 제3의 기관 없이 사용자의 FIDO 인증 정보를 안전하게 공유할 수 있다. 또한, 블록체인으로 공유되는 사용자의 FIDO 인증 정보와 스마트 컨트랙트를 활용해서 FIDO 인증 기능을 블록체인으로 처리할 수 있기 때문에 FIDO 서버 설치 및 유지 관리 비용을 대폭 감소시킬 수 있다.

Ⅲ. 블록체인 기반의 FIDO 범용 인증 시스템

1. 개념 설계

본 시스템의 목적은 블록체인의 기술을 이용하여 공인된 제3의 기관을 이용하지 않고 여러 도메인의 응용 서비스 간에 사용자의 FIDO 인증 정보를 안전하게 공유하고 이용할 수 있게 함으로써, 사용자는 FIDO 등록 과정을 한 번만 수행하고 추가적인 FIDO 등록 절차 없이 모든 사이트에서 FIDO 인증 서비스를 제공받을 수 있는 시스템을 (그림 2)와 같이 제공하는 것이다.



(그림 2) 블록체인 기반의 FIDO 범용 인증 시스템 개념

2. 요구사항

블록체인 기반의 FIDO 범용 인증 시스템을 설계하기 위한 요구사항은 다음과 같다.

가. ID 조회 및 연결

블록체인 기반의 FIDO 범용 인증 시스템은 하나의 블록체인에 사용자의 공개키 정보를 기록하고, 모든 사이트가 사용자의 공개키를 조회하여 이용하는 방식이다. 그래서 블록체인에 기록되어 있는 사용자의 공개키를 식별할 수 있는 정보가 필요하고, 모든 사이트는 그 식별 정보를 확인할 수 있어야 한다. 본고에서는 이 식별 정보를 사용자의 블록체인 ID라고 한다.

일반적으로 모든 사이트가 사용자의 블록체인 ID를 확인할 수 있는 방법은 사용자가 블록체인 ID를 등록하거나, 서비스를 이용하는 시점에서 블록체인 ID를 함께 제공하는 것이다. 하지만 이러한 방식은 사용자에게 추가적인 등록 절차와 인증 정보 관리를 요구하는 것이므로, 본 시스템에서 추구하는 목적을 만족시킬 수 없다. 따라서 본고에서 기술하는 블록체인 기반의 FIDO 범용 인증 시스템은 사용자의 기본 정보인 생년월일과 성별, 디바이스 ID 정보를 활용하여 사용자의 블록체인 ID를 확인하고 블록체인에 기록되어 있는 사용자의 공개키를 조회할 수 있는 방법을 기술한다. 이를 통해서 사용자는 추가적인 등록이나 정보 제공 없이, 기존에 이용하고 있는 사용자 ID만을 이용하여 모든 사이트에서 블록체인 기반의 FIDO 인증 서비스를 제공 받을 수 있다.

나. 독립된 FIDO 정책 관리

블록체인 네트워크에 참여하는 여러 서비스는 독립된 FIDO 정책을 관리할 수 있어야 한다. 이는 블록체인 네트워크를 통해서 FIDO 정책을 동일하게 공유하며 이용할 수 있지만, 사이트마다 FIDO 인증 수단 및 처리 방법을 다르게 운영할 필요가 있다. 예를 들어, FIDO 인증 장치를 특정 회사의 제품만 사용하거나, 복수 개의 FIDO 인증 장치를 등록 또는 인증 과정에서 이용하거

나, 최초 FIDO 인증 후 일정 시간 내에 요청되는 인증에 대해서는 FIDO 인증 장치의 사용자 로컬 인증을 생략하게 하는 등의 정책을 설정할 수 있게 함으로써, 사이트마다 해당 서비스에 맞는 FIDO 인증 서비스를 제공할 수 있도록 한다.

3. 시스템 설계

블록체인 기반의 FIDO 범용 인증 시스템의 구조는 (그림 3)과 같이 사용자 단말과 RP(Relying Party) 서버, FIDO 블록체인으로 구성된다. 기존의 FIDO 서버가 처리했던 FIDO 등록 및 인증에 대한 기능을 블록체인의 스마트 컨트랙트를 통해서 처리하는 구조이다. 그래서 서비스 제공자는 FIDO 서버를 직접 운영할 필요가 없다.

가. 사용자 단말

사용자 단말은 RP 클라이언트와 FIDO 인증 장치로 구성된다. RP 클라이언트는 RP 서버와 통신할 수 있는 앱(응용프로그램)이고, FIDO 인증 장치는 FIDO 등록을 위한 공개키 쌍을 생성 및 FIDO 인증을 위한 전자서명, 키 관리 기능을 수행한다.

나. RP 서버

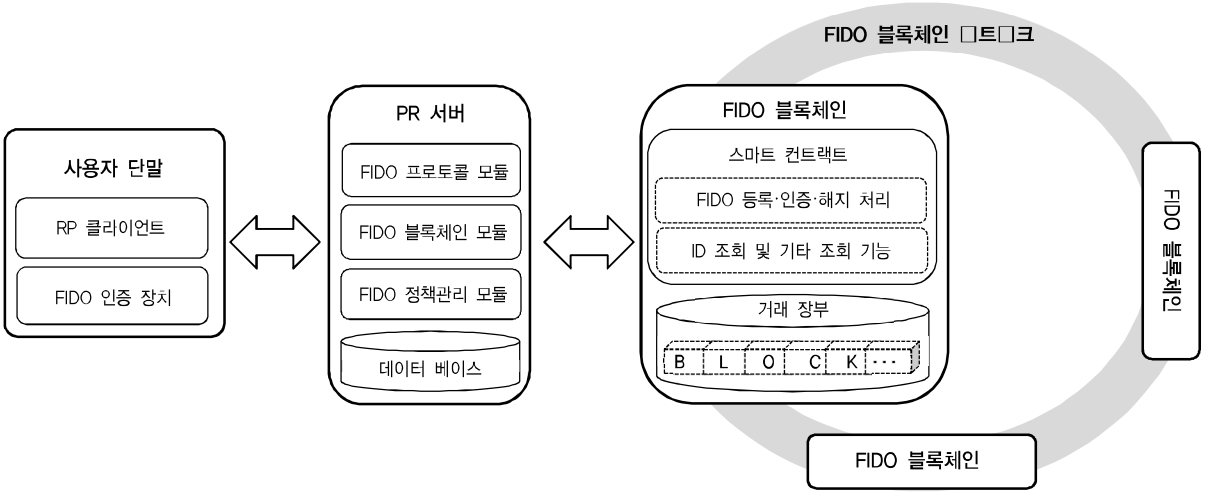
RP 서버는 응용 서비스를 제공하는 서버로 주요 기능은 FIDO 요청 메시지를 생성하고 FIDO 블록체인 모듈을 통해서 FIDO 응답 메시지를 스마트 컨트랙트로 검증한다. 또한, FIDO 정책 관리 모듈을 통해서 독립된 FIDO 요청 메시지를 생성하고 사용자의 계정 정보를 관리하는 데이터베이스로 구성한다.

다. FIDO 블록체인

FIDO 블록체인은 블록체인 네트워크에서 공유되는 거래 장부와 스마트 컨트랙트로 구성된다.

1) 거래 장부

거래 장부는 Key, Value 형태로 구성된 자료구조의 Map과 같은 구조이다. 거래 장부에 기록되는 정보는 FIDO 인증 장치의 메타데이터[10] 정보와 사용자의 FIDO 인증 정보가 〈표 1〉과 같이 기록된다. 〈표 1〉에서 FIDO 인증 장치의 식별자 목록은 FIDO 블록체인에서 이용되는 모든 인증 장치에 대한 목록이고, FIDO 인증 장치의 메타데이터는 FIDO 인증 장치 목록에 기록된 인증 장치에 대한 메타데이터 전문이다. 이 메타데이터는 FIDO 등록 응답 메시지의 신뢰성을 검증하는 데 활



(그림 3) 블록체인 기반의 FIDO 범용 인증 시스템 구조

〈표 1〉 FIDO 블록체인의 거래 장부

구분	속성	내용
FIDO 인증 장치 식별자 목록	Key	– 상수 'AAID'
	Value	– FIDO 인증장치 식별자 리스트
FIDO 인증 장치의 메타데이터	Key	– FIDO 인증장치 식별자
	Value	– FIDO 인증장치의 메타데이터 전문
FIDO 크리덴셜 ID 목록	Key	– 사용자의 블록체인 ID
	Value	– 사용자의 FIDO 크리덴셜 ID 리스트
FIDO 인증 정보	Key	– 사용자의 FIDO 크리덴셜 ID
	Value	– 사용자의 FIDO 인증 정보

〈표 2〉 FIDO 인증 정보

항목	설명
AAID	– 사용자의 FIDO 인증 장치 식별자
Credential ID	– 사용자의 FIDO 크리덴셜 식별자
Attestation	– 사용자의 FIDO 공개키가 포함된 메시지
Sign counter	– 사용자의 FIDO 인증 장치가 서명한 횟수
Registration time	– 사용자의 FIDO 인증 장치가 블록체인 네트워크가 등록되는 최초 등록된 시간
Last authentication time	– 사용자 로컬 인증을 통해서 검증된 FIDO 인증 시간

용된다. FIDO 크리덴셜 목록은 사용자가 등록한 모든 FIDO 크리덴셜 ID 목록이고, 사용자의 블록체인 ID 별로 기록된다. FIDO 크리덴셜 ID 목록은 FIDO 등록 요청 메시지를 생성할 때 활용된다.

FIDO 인증 정보는 사용자의 공개키, FIDO 크리덴셜 정보가 JSON 형태로 구성된 정보이고, 사용자의 FIDO 크리덴셜 ID 별로 기록된다. FIDO 인증 정보는 〈표 2〉와 같고, FIDO 인증 요청 메시지를 생성하거나 FIDO 인증 응답 메시지를 검증할 때 활용된다.

2) 스마트 컨트랙트

스마트 컨트랙트는 프로그래밍 가능한 형태로 구현된 블록체인이고 참여자 누구나 검증할 수 있다. 그래서 스마트 컨트랙트를 통해서 블록체인에 기록되는 정보는 공인된 제3자가 없어도 강력한 신뢰성을 담보한다.

블록체인 기반의 FIDO 범용 인증 시스템을 구성하는 스마트 컨트랙트는 〈표 3〉과 같다. 주요 기능에 대한 설명과 처리 로직은 다음과 같다.

• queryUserCredentialIds

블록체인에 기록되어 있는 사용자의 모든 FIDO 크리덴셜 ID 목록을 조회한다.

① 상수 'AAID'를 Key 값으로 하여 FIDO 인증 장치의 식별자 목록을 조회한다.

② 조회된 FIDO 인증 장치의 식별자 수만큼 블록체인 ID를 생성한다. 블록체인 ID은 userHash 정보와 FIDO 인증 장치의 식별자 정보를 연결하고, 연결된 문자열을 해쉬(Hash)한 결과이다. userHash 정보는 스마트 컨트랙트의 Input 데이터이며, RP 서버에 의해서 생성된다. RP 서버는 사용자의 생년월일과 성별, RP 클라이언트가 설치된 사용자의 디바이스 ID 정보를 연결하고, 연결된 문자열을 해쉬하여 userHash 정보를 생성한다.

③ 생성된 모든 블록체인 ID를 Key 값으로 하여 사용자의 FIDO 크리덴셜 ID 목록을 조회하고, 조회된 모든 FIDO 크리덴셜 ID를 반환한다.

• queryUserCredentials

블록체인에 기록되어 있는 사용자의 모든 FIDO 인증 정보를 조회한다.

① 스마트 컨트랙트 queryUserCredentialIds를 이용하여 모든 FIDO 크리덴셜 ID를 조회한다.

② 조회된 모든 FIDO 크리덴셜 ID를 Key 값으로 하여 FIDO 인증 정보를 조회하고, 조회된 FIDO 인증 정보를 모두 반환한다.

• queryUserBlockChainId

사용자의 블록체인 ID를 조회한다.

① Input 데이터인 FIDO 크리덴셜 ID를 Key 값으로 하여 FIDO 인정 정보를 조회한다.

② 조회된 FIDO 인증 정보에서 FIDO 인증 장치의 식별자인 AAID(Authenticator Attestation ID)

〈표 3〉 FIDO 블록체인의 스마트 컨트랙트

No	Smart Contract API		Parameters	
1	queryUserCredentialIds	Input	userHash	– 사용자의 기본 정보를 해쉬한 정보
		Output	userCredentialIdList	– 사용자의 FIDO 크리덴셜 ID 목록
2	queryUserCredentials	Input	userHash	– 사용자의 기본 정보를 해쉬한 정보
		Output	userCredentialInfoList	– 사용자의 FIDO 인증 정보 목록
3	queryUserBlockChainId	Input	userHash	– 사용자의 기본 정보를 해쉬한 정보
			credentialId	– 사용자의 FIDO 크리덴셜 ID
		Output	userBlockChainId	– 사용자의 블록체인 ID
4	registerCredential	Input	userHash	– 사용자의 기본 정보를 해쉬한 정보
			attestation	– FIDO 등록 응답 메시지
		Output	True/False	– FIDO 등록 성공 여부
5	verifyCredential	Input	isGesture	– FIDO 인증 장치의 명시적인 사용자 인증 처리 여부
			assertion	– FIDO 인증 응답 메시지
		Output	True/False	– FIDO 인증 성공 여부
6	deleteUserCredential	Input	userBlockChainId	– 사용자의 블록체인 ID
			credentialId	– 사용자의 FIDO 크리덴셜 ID
		Output	True/False	– 사용자의 FIDO 인증 정보 삭제 성공 여부
7	registerMetadata	Output	metadataStement	– FIDO 인증 장치의 메타데이터 전문
		Input	True/False	– FIDO 인증 장치의 메타데이터 등록 성공 여부
8	deleteMetadata	Input	aaid	– FIDO 인증 장치의 식별자
		Output	True/Fase	– FIDO 인증 장치의 메타데이터 삭제 성공 여부

정보를 확인하고, 확인된 AAID 정보와 Input 데이터인 userHash 정보를 연결하고, 연결된 문자열을 해쉬한 결과를 반환한다.

• registerCredential

FIDO 등록 응답 메시지인 attestation을 검증하고, 검증된 사용자의 FIDO 인증 정보를 거래 장부에 기록한다.

⓪ Input 데이터인 attestation 메시지에서 AAID 정보를 확인하고, 확인된 AAID 정보를 Key 값으로 하여 해당 FIDO 인증 장치의 메타데이터를 조회한다.

⓪ 조회된 메타데이터 전문에서 attestation의 신뢰성을 검증할 수 있는 FIDO 인증 장치의 공개키 정보를 확인하고, 확인된 공개키 정보를 통해서 attestation의 서명을 검증한다.

⓪ 검증이 완료되면, attestation 메시지에서 FIDO 크리덴셜 ID를 확인하고, 사용자의 FIDO 인증 정보를 생성한다. 생성된 FIDO 인증 정보는 〈표 1〉의 FIDO 인증 정보 형태로 기록한다.

⓪ FIDO 인증 정보 기록이 완료되면, 사용자의 블록체인 ID를 생성한다. 블록체인 ID는 Input 데이터인 userHash 정보와 attestation 메시지에서 확인한 AAID 정보를 이용해서 생성한다. 그리고 attestation 메시지에서 확인한 FIDO 크리덴셜 ID를 〈표 1〉의 FIDO 크리덴셜 목록 형태로 기록한다.

• verifyCredential

FIDO 인증 응답 메시지인 assertion 검증하고, 블록체인에 기록되어 있는 사용자의 FIDO 인증 정보를 업데이트 한다.

⓪ Input 데이터인 assertion 메시지에서 FIDO 크

리덴셜 ID 정보를 확인하고, 확인된 FIDO 크리덴셜 ID를 Key 값으로 하여 사용자의 FIDO 인증 정보를 조회한다.

⓪ 사용자의 FIDO 인증 정보에 포함되어 있는 사용자의 FIDO 인증 공개키를 확인하고, 확인된 공개키를 통해서 assertion의 서명을 검증한다.

⓪ 검증이 완료되면, assertion 메시지를 이용하여 사용자의 FIDO 인증 정보를 업데이트 한다. 업데이트 정보는 서명 횟수 정보와 인증 시간 정보이다. 인증 시간 정보는 Input 데이터인 isGesture 정보가 True인 경우에만 현재 시간으로 업데이트한다.

• deleteUserCredential

블록체인에 기록되어 있는 사용자의 모든 FIDO 크리덴셜 정보를 삭제한다.

⓪ Input 데이터인 FIDO 크리덴셜 ID를 Key 값으로 하여 사용자의 FIDO 인증 정보를 Null로 업데이트 한다.

⓪ Input 데이터인 블록체인 ID를 Key 값으로 하여 FIDO 크리덴셜 ID 목록 조회하고, Input 데이터인 FIDO 크리덴셜 ID를 목록에서 삭제하고, 삭제된 목록을 업데이트한다.

Ⅳ. 블록체인 기반의 FIDO 범용 인증 시나리오

본 장에서는 블록체인의 거래 장부와 스마트 컨트렉트를 활용하여 FIDO 등록 및 인증 과정을 기술한다.

또한, FIDO 인증 과정에서 사용자의 서비스 ID만으로 사용자의 블록체인 ID를 확인하고, 거래 장부에 기록된 사용자의 FIDO 공개키를 조회하여 FIDO 인증을 처리하고 ID를 연결할 수 있는 방법을 설명한다.

1. FIDO 등록

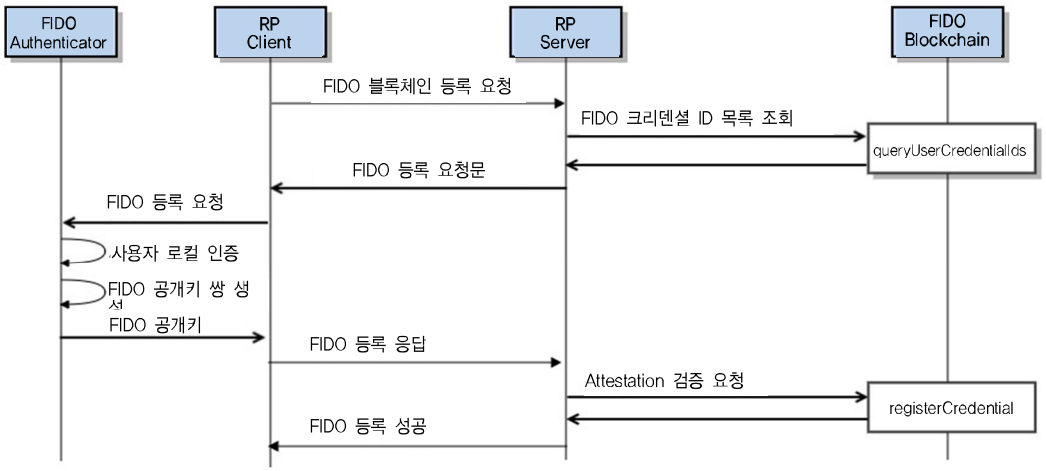
FIDO 등록은 사용자의 FIDO 인증 장치를 FIDO 블록체인에 등록하는 과정이며, 더 명확하게는 FIDO 인증 장치가 생성한 공개키 쌍 중에서 공개키를 블록체인에 기록하는 것이다. (그림 4)는 블록체인 기반의 FIDO 등록 과정을 도식화한 것이고, 과정에 대한 설명은 다음과 같다.

⓪ FIDO 블록체인 등록 요청

– 사용자가 RP 클라이언트를 이용하여 FIDO 등록을 요청한다. 사용자의 서비스 ID와 사용자 단말의 디바이스 ID를 함께 제공한다.

⓪ 사용자의 FIDO 크리덴셜 ID 목록 조회

– RP 서버는 queryUserCredentialIds를 이용하여 FIDO 크리덴셜 ID 목록을 확인한다.



(그림 4) 블록체인 기반의 FIDO 등록 처리 흐름도

⑨ FIDO 등록 요청문 생성

- RP 서버는 조회된 FIDO 크리덴셜 ID 정보와 RP 서버가 독자적으로 운용하는 등록 정책 정보를 활용하여 FIDO 등록 요청문을 생성하고 RP 클라이언트에 전송한다.
- FIDO 등록 요청문을 생성할 때, FIDO 크리덴셜 ID 정보는 disallowed 옵션으로 설정된다. 이 옵션은 동일한 사용자의 FIDO 인증 장치가 재등록 되는 것을 방지한다.

⑩ FIDO 등록 요청 및 응답

- RP 클라이언트는 FIDO 인증 장치에 FIDO 등록을 요청하고, FIDO 인증 장치는 disallowed 옵션에 포함된 FIDO 크리덴셜 ID가 FIDO 인증 장치에서 관리하는 FIDO 크리덴셜 ID 목록에 존재하는지 확인한다. 만약 존재한다면 등록 요청 거부 메시지를 발생시키거나, 향후 새롭게 생성된 공개키 쌍으로 업데이트한다.
- 만약 존재하지 않는다면, FIDO 인증 장치는 인증 장치가 제공하는 인증 수단을 통해서 사용자의 로컬 인증을 수행한다. 정상적으로 로컬 인증이 완료되면 FIDO 등록을 위한 공개키 쌍을 생성한다. 생성된 공개키 쌍 중에서 공개키는 RP 클라이언트에게 전송한다.
- RP 클라이언트는 FIDO 인증장치로부터 전달받은 사용자의 공개키를 포함한 attestation을 생성하고, RP 서버에 전송한다.

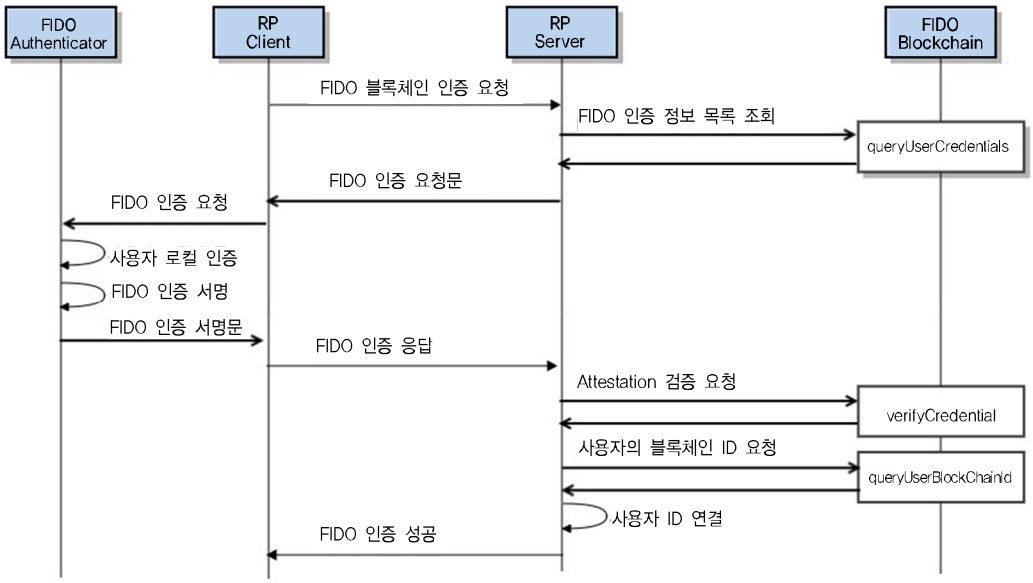
⑪ attestation 검증

- RP 서버는 attestation 메시지에서 FIDO 크리덴셜 ID 정보와 AAID 정보를 확인하고, registerCredential를 통해서 assertion을 검증한다.
- 검증이 완료되면, RP 서버는 RP 클라이언트에게 FIDO 등록 성공 메시지를 전송한다.

2. FIDO 인증 및 ID 연결

FIDO 인증은 FIDO 인증 장치가 개인키로 서명한 서명문을 블록체인에 등록된 사용자의 공개키로 검증하는 것이다. (그림 5)는 FIDO 인증 과정을 도식화한 것이고, 과정에 대한 설명은 다음과 같다.

① FIDO 블록체인 인증 요청은 FIDO 블록체인 등록 과정과 동일하다.



(그림 5) 블록체인 기반의 FIDO 인증과정 흐름도

⓪ 사용자의 FIDO 인증 정보 조회

- RP 서버는 queryUserCredentials를 이용하여 사용자의 FIDO 인증 정보를 확인한다.

⓪ FIDO 인증 요청문 생성

- RP 서버는 사용자의 FIDO 인증 정보와 RP 서버가 독립적으로 관리하는 인정 정책 정보를 활용하여 FIDO 인증 요청문을 생성하고 RP 클라이언트에게 전송한다.
- FIDO 인증 요청문을 생성할 때, 사용자의 FIDO 인증 정보 중에서 FIDO 크리덴셜 ID는 allowed 옵션으로 설정된다. 이 옵션은 allowed 옵션에 있는 FIDO 크리덴셜 ID와 관련된 FIDO 인증 장치만 해당 요청에 대한 응답을 처리할 수 있게 한다. 즉, 사용자의 FIDO 등록 과정에서 사용된 FIDO 인증 장치를 선택할 수 있는 기능이다. 이 옵션을 통해서 사용자가 블록체인 ID를 제공하지 않아도 블록체인 기반의 FIDO 인증을 처리할 수 있다.

⓪ FIDO 인증 요청 및 응답

- RP 클라이언트는 FIDO 인증장치에 FIDO 인증을 요청하고, FIDO 인증장치는 allowed 목록에 있는 FIDO 크리덴셜 ID가 FIDO 인증장치에서 관리하고 있는 FIDO 크리덴셜 ID 목록에 존재하는지 확인한다. 만약 존재하지 않는다면, 인증 요청 거부 메시지를 발생시킨다.
- 존재한다면, FIDO 인증장치는 인증장치가 제공하는 인증 수단을 통해서 사용자의 로컬 인증을 수행한다. 정상적으로 로컬 인증이 완료되면 FIDO 인증을 위한 서명문을 생성하고, FIDO 인증 서명문을 RP 클라이언트에게 전송한다.
- RP 클라이언트 FIDO 인증장치로부터 전달받은 FIDO 인증 서명문을 포함한 assertion을 생성하고 RP 서버에 전송한다.

⓪ assertion 검증 및 ID 연결

- RP 서버는 assertion 메시지에서 FIDO 크리덴셜 ID 정보를 확인하고, verifyCrednetial을 통해서 assertion을 검증한다.
- 검증이 완료되면, RP 서버는 queryUserBlockChainId를 통해서 사용자의 블록체인 ID를 조회하고, 확인된 사용자의 블록체인 ID를 사용자의 서비스 ID와 연결하여 데이터베이스에 저장하고, RP 클라이언트에게 인증 성공 메시지를 전송한다.

V. 결론

2018년 FIDO 2.0 표준이 완료되면, 현재 금융권을 중심으로 모바일 환경에서 활용되고 있는 FIDO 인증 기술이 웹 또는 PC 기반의 응용 서비스의 사용자 인증 기술로 활용될 것이다. 사용자는 지금보다 훨씬 더 많은 FIDO 인증 서비스를 이용하게 되고, 반복되는 FIDO 등록 절차가 사용자의 편의성을 저해할 수 있다.

본고에서 여러 도메인의 응용 서비스 간에 사용자의 FIDO 인증 정보를 서버 없이 공유할 수 있는 블록체인 기반의 FIDO 범용 인증 시스템은 기술하였다. 본 시스템의 특징은 모든 응용 서비스의 사용자 ID만을 이용하여 블록체인에 기록되어 있는 사용자의 FIDO 인증 정보를 조회할 수 있는 ID 연결 방식이다. 이를 통해서 사용자는 FIDO 등록 과정을 한 번만 수행하고 추가적인 FIDO 등록 과정 없이 타 응용 서비스의 FIDO 인증 서비스를 이용할 수 있고, 서비스 제공자는 공인된 제3의 기관을 이용하지 않고 사용자의 FIDO 인증 정보를 안전하게 공유하고 활용할 수 있기 때문에 FIDO 서버 설치 및 유지 관리 비용을 절감할 수 있을 것으로 기대한다.

용어해설

소셜 로그인 포탈 사이트나 소셜네트워크서비스 계정으로 다른 회사의 서비스나 앱(응용프로그램)을 자유롭게 이용할 수 있는 서비스.

크리덴셜(Credential) 자격을 증명하는 토큰으로, 사용자(클라이언트)가 서버로부터 허가된 사용자임을 증명할 수 있는 정보이다[11].

약어 정리

AAID	Authenticator Attestation ID
FIDO	Fast Identity Online
RP	Relying Party

참고문헌

[1] 김태균, "네이버 아이디로 로그인 사용자 월 1천만명 넘어," 연합뉴스, 2017. 6. 2.

[2] 정영훈, "온라인 서비스에서의 소셜 로그인과 소비자 이슈," 소비자정책동향, 제 79호, 한국소비자원, 2017. 4. 30, pp. 1-19.

[3] T.S. Pasricha, "Pros and Cons of Facebook Social Login on eCommerce Website," nopAccelerate, Sept. 19, 2017, Accessed 2017. http://www.nopaccelerate.com/pros-cons-facebook-social-login-ecommerce-website/

[4] ITWorld 편집부, "FIDO 생체인증 플랫폼 도입 예정 기업 급증," ITWorld, 2016. 10. 27, Accessed 2017. http://www.itworld.co.kr/news/101780

[5] FIDO Alliance, *History of FIDO Alliance*, 2017, Accessed 2017. https://fidoalliance.org/about/history/

[6] 조상래, 김수형, "FIDO 기술 표준화 동향," TTA 저널, vol. 172, 2017. 10, pp. 65-70.

[7] W3C, *Web Authentication: An API for accessing Public Key Credentials Level 1*, Dec. 5, 2017, Accessed 2017. https://www.w3.org/TR/webauthn/

[8] 김석현, 조영섭, 조상래, 김수형, "FIDO UAF 1.0 서버 구현," 한국정보처리학회 추계 학술대회, 2015. 4, pp. 620-623.

[9] Wikipedia, *Blockchain*, 2017, Accessed 2017. https://en.wikipedia.org/wiki/Blockchain

[10] FIDO Alliance, *FIDO Metadata Statements*, 2017, Accessed 2017. https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-metadata-statement-v1.1-id-20170202.html

[11] 최종원, 이정현, "안드로이드 구글 계정 앱의 개인정보 유출 취약점 분석," 디지털포렌식연구, 제8권 제2호, 2014. 12, pp. 65-81.