TTA Standard

정보통신단체표준(국문표준) 제정일: 2018 년 xx 월 xx 일

TTAx.xx-xx.xxxx/R1

블록체인 기반의 FIDO 범용 인증 프레임워크 요구사항

Requirements for FIDO Universal Authentication Framework Based on Blockchain

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회	개인정보보호/ID관리, 블록체인 보안 프로젝트그룹 (PG502)
표준안 심의 위원회	정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	김석현	ETRI	선임	-	-
표준 초안 작성자	김석현	ETRI	선임	-	-
	조상래	ETRI	책임	-	-
	조영섭	ETRI	책임	-	-
사무국 담당	박수정	TTA	책임	-	-

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 2018.xx

서 문

1 표준의 목적

본 표준은 블록체인 기반으로 구성된 FIDO 범용 인증 프레임워크에 대한 필요성 및 요구사항을 정의한다. 블록체인 기반의 FIDO 범용 인증 프레임워크는 블록체인으로 연결된 모든 서비스가 공인된 제 3의 기관 없이 서로 다른 도메인 간에 사용자의 FIDO 인증정보를 안전하게 공유하고 이용할 수 있는 시스템이다. 또한 사용자는 FIDO 등록 절차를 한번만 수행하면 추가적인 FIDO 등록 절차 없이 언제 어디서나 블록체인으로 연결된 모든 도메인에서 FIDO 인증 서비스를 제공받을 수 있다.

2 주요 내용 요약

본 표준은 블록체인 기반의 FIDO 범용 인증 프레임워크에 대한 필요성과 요구사항을 정의하고, 블록체인으로 연결된 모든 도메인에서 사용자의 FIDO 인증정보를 안전하게 공유할 수 있는 ID 연결 방법을 설명한다. 그리고 공유되는 FIDO 인증정보를 이용한 블록체인 기반의 FIDO 범용 인증 방법을 기술한다.

3 인용 표준과의 비교

해당 사항 없음

3.1 인용 표준과의 관련성

해당 사항 없음

3.2 인용 표준과 본 표준의 비교표

해당 사항 없음

Preface

1 Purpose

This standard defines the need and requirements of a blockchain-based FIDO universal authentication framework. The blockchain-based FIDO universal authentication framework is a system in which all services connected to the blockchain can securely share and use the user's FIDO credentials between different domains without an authorized third party. In addition, the user can receive the FIDO authentication service anytime and anywhere without additional FIDO registration procedure once the FIDO registration procedure is performed.

2 Summary

This standard defines the need and requirements for a blockchain-based FIDO universal authentication framework and describes the ID-Mapping method in which all nodes connected by a blockchain can securely share the user's FIDO credentials. In addition, this standard describes the methods of blockchain-based FIDO authentication services using the shared FIDO credentials.

3 Relationship to Reference Standards

None

목 차

블록체인 기반의 FIDO 범용 인증 프레임워크 요구사항

(Requirements for FIDO Universal Authentication Framework Based on Blockchain)

1 적용 범위

본 표준은 블록체인 기반의 FIDO 범용 인증 프레임워크에 대한 필요성 및 요구사항을 정의한다. 그리고 사용자의 FIDO 인증정보를 블록체인에 참여하는 모든 노드가 조회하고 이용하기 위한 블록체인 ID 연결 방법을 제안하고, 이를 통한 블록체인 기반의 FIDO 범용 인증 방법을 설명한다. 그리고 기존의 FIDO 범용 인증 시스템 대비 블록체인 기반의 FIDO 범용 인증 프레임워크가 사용자 측면에서 향상된 서비스 요소를 설명한다.

본 표준은 블록체인의 프라이빗(Private) 환경으로 구성되는 노드에 대한 기능 요구사항을 정의하고 사용자 단말에 대한 요구사항은 포함하지 않는다.

본 표준은 접근이 제한된 Private 환경 내의 인증 받은 노드들만 구성되어 있으며, Public한 블록체인 환경은 본 표준의 범위에 포함되지 않는다.

2 인용 표준

해당사항 없음

3 용어 정의

3.1 FIDO 인증 (Fast Identity Online) [1]

온라인 환경에서 패스워드 대신 생체 정보를 활용하여 빠르고 안전하게 사용자를 인증할 수 있는 범용 인증 플랫폼

3.2 AAID (Authenticator attestation ID) [2]

FIDO 인증장치에 대한 제조사 및 모델을 표현할 수 있는 식별자 정보. 일반적으로 FIDO UAF 인증장치인 경우에는 AAID로 표현하고, FIDO2 인증장치는 AAGUID로 표현함

3.3 메타데이터 명세서

FIDO 인증장치에 대한 암호 처리 방식, 사용자 인증 방식, 암호키 보호 및 매칭 방법 등 인증장치의 다양한 기능을 기술한 명세서. 서버가 해당 인증장치에 대한 신뢰성을 검증하는데 필요한 정보를 포함함

3.4 Same Origin Policy (동일 출처 정책) [3]

한 출처(Origin)에서 로드된 문서나 스크립트가 다른 출처 자원과 상호작용하지 못하도록 제약하는 정책이고, 출처는 URL에서 스킴(scheme), 호스트(host), 포트(port)로 정의한 정보임

3.5 크리덴셜 (Credentila) [TTAK.KO-12.0292]

신원이나 자격을 주장하면서 증거로 제출된 데이터 집합이며, 본 표준에서는 사용자의 FIDO 인증정보를 의미함

3.6 블록체인 (Blockchain) [4]

온라인 금융 거래 정보를 블록으로 연결하여 P2P 네트워크 분산 환경에서 중앙 관리 서버가 아닌 참여자들의 개인 디지털 장비에 분산·저장시켜 공동으로 관리하는 기술

3.7 스마트 컨트랙트(Smart Contract) [5]

블록체인에서 거래의 일정 조건을 만족시키면 당사자 간에 자동으로 거래가 체결되도록 하는 기술

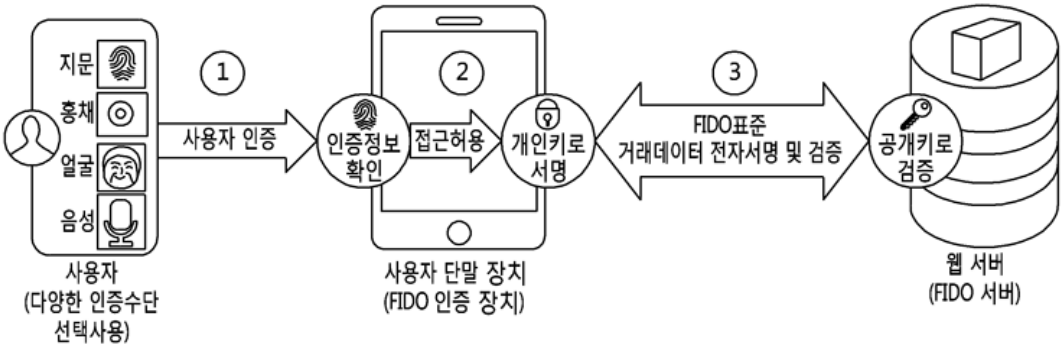
4 약어

AAGUID	Authenticator attestation GUID
UAF	Universal Authentication Framework
U2F	Universal 2nd Factor authentication
RPID	Relying Party ID
SOP	Same Origin Policy

5 블록체인 기반의 FIDO 범용 인증 프레임워크 필요성

5.1 기존의 FIDO 인증 시스템

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 그림 5-1과 같이 사용자 인증을 위한 공개키를 서버에 등록하는 과정이 필요하다. 향후 FIDO 인증 시스템을 도입하는 서비스가 증가할수록 사용자는 반복적인 FIDO 등록 과정을 요구 받게 되는 불편이 야기될 수 있다.

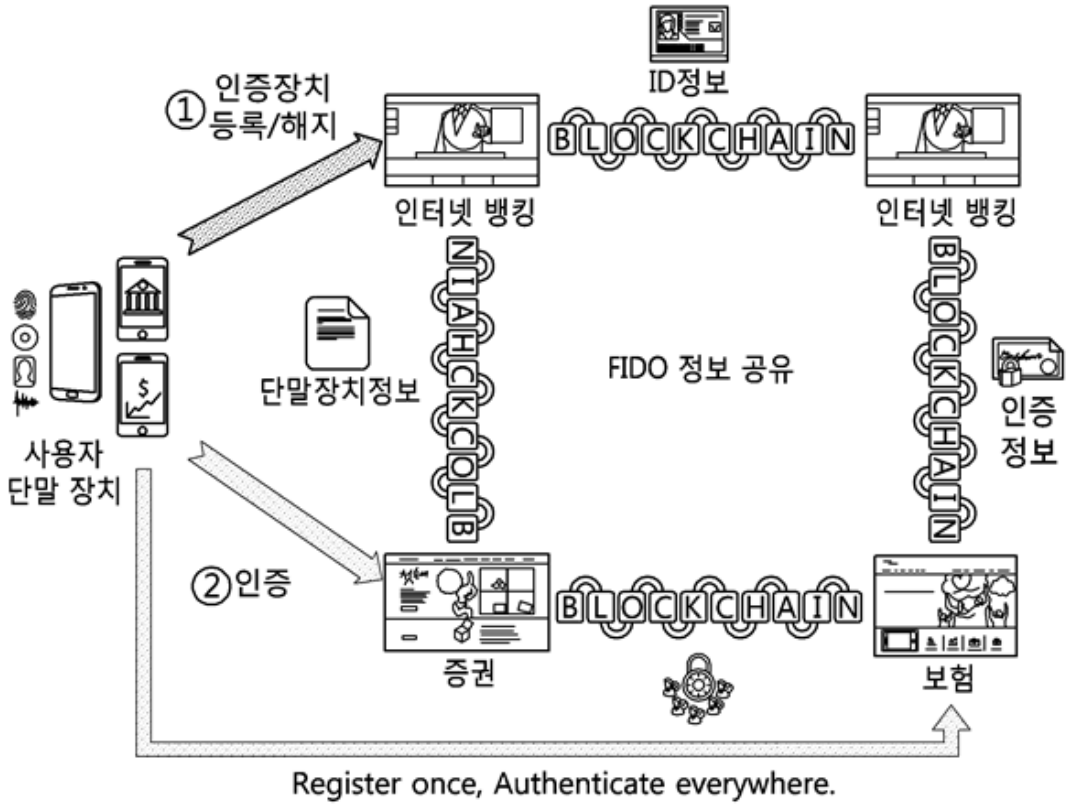


(그림 5-1) FIDO 인증 기술 개념도 [6]

5.2 블록체인 기반의 FIDO 범용 인증 프레임워크

본 표준은 FIDO 인증 기능을 블록체인 환경에서 운영하기 위한 블록체인 기반의 FIDO 범용 인증 프레임워크에 대한 요구사항을 정의한다.

블록체인 기반의 FIDO 범용 인증 프레임워크는 공인된 제 3의 기관이 개입하지 않고 서로 다른 도메인의 응용 서비스 간에 사용자의 FIDO 인증정보를 안전하게 공유하고 이용할 수 있는 시스템이다. 이를 통해, 사용자는 한번만 FIDO 등록을 수행하면 블록체인으로 연결된 모든 서비스에 대해서 추가적인 사용자의 FIDO 등록 절차 없이 FIDO 인증 서비스를 제공 받을 수 있다. 그림 5-2는 블록체인 기반의 FIDO 범용 인증 시나리오를 나타낸다.



(그림 5-2) 블록체인 기반의 FIDO 범용 인증 시나리오 [6]

5.3 기존의 FIDO 인증 시스템 대비 효율성

블록체인 기반의 FIDO 범용 인증 프레임워크는 FIDO 등록을 한 번만 수행하면 추가적인 FIDO 등록 절차 없이 블록체인에 참여하는 모든 응용 서비스에서 FIDO 인증 서비스를 이용할 수 있다. 그러므로 서비스 제공자는 공인된 제 3의 기관을 이용하지 않고 사용자의 FIDO 인증정보를 안전하게 공유하고 활용할 수 있어 기존의 FIDO 시스템 대비 시스템 운용을 위한 유비 및 보안 관리 등에서 비용을 절감할 수 있는 효과가 있다.

표 5-1은 기본 FIDO 인증 시스템 대비 블록체인 기반의 FIDO 범용 인증 프레임워크의 효율적 측면을 정리한 것이다.

<표 5-1> FIDO 인증 시스템과 블록체인 기반의 FIDO 범용 인증 프레임워크 비교

구분	FIDO 인증	블록체인 기반의 FIDO 범용 인증 프레임워크
등록 기준	서비스 (매번 등록)	블록체인 네트워크 (한번 등록)
인증 세션	공유 불가	공유 가능
운영 비용	FIDO 서버 및 DB 운영 (높음)	FIDO 서버의 검증 기능 및 인증 정보 공유 (낮음)

6 블록체인 기반의 FIDO 범용 인증 프레임워크 요구사항

6.1 단일 도메인 운영

본 표준에서는 따르고 있는 웹 인증 기술은 웹 Origin 정보를 응용 서비스의 식별자 정보로 사용한 Same-Origin-Policy(SOP) 정책을 준수하고 있다. 그래서 FIDO 인증장치는 사용자의 FIDO 인증정보를 응용 서비스의 식별자 정보인 웹 Origin과 연결하여 관리하고 있다. 그러므로 본 표준에서 정의한 블록체인 기반의 FIDO 범용 인증 프레임워크는 블록체인으로 구성되어 있는 모든 노드가 블록체인으로 공유되는 하나의 FIDO 인증정보를 이용하기 위해서 단일 도메인으로 구성되어야 하는 설계 요구 사항이 필요하다.

예를 들어, 은행, 증권, 보험과 같이 3개의 업체가 블록체인 기반의 FIDO 범용 인증 프레임워크를 구성해서 FIDO 인증 서비스를 제공한다고 가정하자. FIDO 인증 서비스 제공을 위해서 공통으로 사용할 도메인(ex, blockchain.com)을 기준으로 블록체인에 참여하는 각 업체들은 각자의 서브 도메인을 다음과 같이 생성하고 사용하게 되면, 은행을 통해서 등록한 FIDO 인증정보를 증권에서 이용할 수 있게 된다.

은행 - bank.blockchain.com

증권 - stock.blockchain.com

보험 - insurance.blockchain.com

6.2 FIDO 인증장치의 메타데이터 명세서 관리

블록체인 기반의 FIDO 범용 인증 프레임워크를 구성하고 운영하기 위해서는 FIDO 인증 서비스를 제공할 FIDO 인증장치에 대한 메타데이터 명세서가 블록체인으로 공유되어야 하는 기능 요구사항이 필요하다.

FIDO 인증장치의 메타데이터 명세서에는 FIDO 인증장치가 생성하고 블록체인에 등록하는 크리덴셜에 대한 신뢰성을 검증할 수 있는 공개키 인증서와 같은 정보가 포함되어야 한다. 이 공개키 인증서는 블록체인 기반의 FIDO 범용 인증 시스템이 허가한 FIDO 인증장치가 FIDO 등록을 올바르게 요청했는지 확인하는데 사용된다. 그러므로 블록체인에 참여하는 모든 노드가 블록체인으로 공유되는 FIDO 인증장치의 메타데이터 명세서를 관리할 수 있는 기능이 필요하다.

6.3 FIDO 범용 인증 스마트 컨트랙트

본 표준에서 정의한 블록체인 기반의 FIDO 범용 인증 프레임워크를 구성하고 운영

하기 위해서는 블록체인에 참여하는 모든 노드가 블록체인에 기록되는 모든 정보에 대해서 합의하는 과정이 필요하다. 그렇지 않으면 블록체인을 공유되는 정보에 대한 신뢰성을 보장할 수 없다. 그래서 블록체인에 참여하는 모든 노드가 동일한 FIDO 검증 기능을 공유하고 실행할 수 있는 스마트 컨트랙트가 필요하다.

6.3.1 FIDO 인증장치의 메타데이터 명세서 관리

블록체인에 참여하는 모든 노드들은 블록체인으로 공유되는 FIDO 인증장치에 대한 메타데이터 명세서 등록, 중복 등록 여부 확인, 업데이트, 삭제 등의 기능이 필요하다. 또한 블록체인에 FIDO 인증장치의 메타데이터가 기록된다는 의미는 블록체인 기반의 FIDO 범용 인증 시스템에서 해당 FIDO 인증장치의 사용을 허용한다는 의미이므로, 블록체인에 참여하는 모든 노드들로부터 해당 FIDO 인증장치에 대한 사용 여부에 대한 합의를 수행하는 스마트 컨트랙트가 필요하다.

6.3.2 FIDO 등록

사용자의 FIDO 등록 요청은 블록체인에 참여하고 있는 하나의 노드를 통해서 이루어 질 것이다. 만약 FIDO 등록을 해당 노드에서만 검증하고 블록체인을 통해서 사용자의 FIDO 인증정보를 공유한다면, 블록체인에 참여하고 다른 노드들이 그 정보를 이용하기에는 신뢰성이 부족하다. 그러므로 블록체인에 참여하고 있는 모든 노드가 스마트 컨트랙트를 통해서 FIDO 등록 응답을 모두 동시에 검증하고, 검증 결과가 모두 동일할 경우에만 사용자의 FIDO 인증정보를 블록체인에 기록해야 한다.

6.3.3 FIDO 인증

블록체인에 참여하고 있는 모든 노드가 스마트 컨트랙트를 통해서 FIDO 인증 응답을 동시에 검증하고, 검증 결과가 모두 동일한 경우에만 블록체인에 기록되어 있는 사용자의 FIDO 인증정보를 업데이트해야 한다. 업데이트되는 정보는 다음 FIDO 인증 과정에서 중요한 보안 검증 요소로 활용되기 때문에 모든 노드들 간의 합의가 필요하다.

6.3.4 FIDO 해지

블록체인에 참여하고 있는 모든 노드가 스마트 컨트랙트를 통해서 기 등록된 사용자의 FIDO 인증정보를 삭제할 수 있는 기능이 필요하다. 삭제를 위한 스마트 컨트랙트

는 삭제하려고 하는 사용자의 FIDO 인증정보에 대한 소유자를 확인하고 삭제해야 한다.

소유자 확인 방법은 사용자의 FIDO 인증정보를 통한 FIDO 인증 절차를 수행하는 것으로 확인이 가능하며, FIDO 해지를 위한 스마트 컨트랙트는 사용자의 FIDO 인증정보에 대한 소유자 확인 후에 실행되어야 한다.

6.4 사용자의 FIDO 인증정보 공유를 위한 블록체인 ID

블록체인 기반의 FIDO 범용 인증 프레임워크는 블록체인 네트워크에 사용자의 FIDO 인증정보를 한번만 기록하고, 블록체인에 참여하는 모든 노드들이 사용자의 FIDO 인증정보를 조회하여 이용하는 방식이다. 그래서 블록체인에 기록되어 있는 사용자의 FIDO 인증정보를 식별할 수 있는 정보가 필요하며 모든 참여 노드들이 그 식별 정보를 확인할 수 있는 방법이 필요하다. 본 표준에는 그 식별 정보를 블록체인 ID라고 한다.

6.5 독립된 FIDO 범용 인증 정책 관리

블록체인 네트워크에 참여하는 모든 노드들은 각각 제공하는 응용 서비스가 다를 수 있다. 그러므로 독립된 FIDO 정책 관리를 통해서 응용 서비스에 맞는 FIDO 인증 수단 및 처리 방법을 설계할 수 있는 방법이 필요하다.

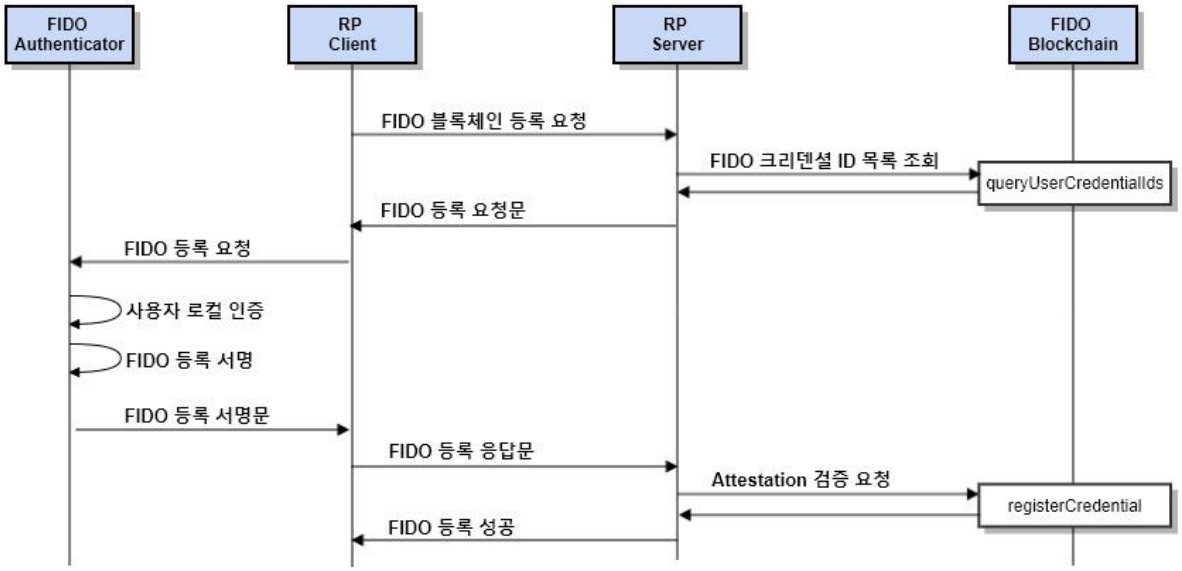
예를 들어, 특정 회사의 FIDO 인증장치만 사용하거나, 복수 개의 FIDO 인증장치를 등록해서 멀티 인증 서비스를 제공하거나, 일정 시간 내에 요청되는 FIDO 인증에 대해서는 FIDO 인증장치의 사용자 로컬 인증을 생략하게 하는 등의 정책을 설정할 수 있는 기능이 요구될 수 있다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

블록체인 기반의 FIDO 등록

FIDO 등록은 사용자의 FIDO 인증장치를 블록체인에 등록하는 과정이며, 더 명확하게는 FIDO 인증장치가 생성한 공개키 쌍 중에서 공개 키를 블록체인에 기록하는 것이다. 본 표준에서는 사용자의 FIDO 인증정보를 크리덴셜으로 표현하며, 크리덴셜 ID는 FIDO 인증정보에 포함되어 있는 사용자의 공개키 식별자 정보이다. 아래 그림은 블록체인 기반의 FIDO 등록 과정을 도식화한 것이다.



(부록 I-1) 블록체인 기반의 FIDO 등록 흐름 [6]

1. FIDO 블록체인 등록 요청
   A. FIDO 인증장치가 탑재 또는 연결되어 있는 디바이스 ID 정보와 사용자의 생년월일, 성별 정보를 RP 서버에 전달한다. 또는 디바이스 ID와 서비스 ID만을 전달할 수 있다.
2. 사용자의 FIDO 크리덴셜 ID 목록 조회
   A. RP 클라이언트로부터 전달 받은 정보를 이용해서 블록체인 ID를 생성한다. 만약 서비스 ID를 전달 받았다면, RP 서버는 서비스 ID로 기 등록 되어 있는 사용자의 생년월일과 성별 정보를 이용해서 블록체인 ID를 생성한다.
   B. 스마트 컨트랙트를 이용해서 블록체인에 기록되어 있는 사용자의 FIDO 크리덴셜 ID 목록을 조회한다. 조회를 위해서 블록체인 ID를 이용한다.
3. FIDO 등록 요청문 생성
   A. 조회된 사용자의 FIDO 크리덴셜 ID들은 disallowed 옵션으로 설정하고

FIDO 등록 요청 메시지를 생성한다. disallowed 옵션은 FIDO 중복 등록을 방지하기 위한 옵션이다.

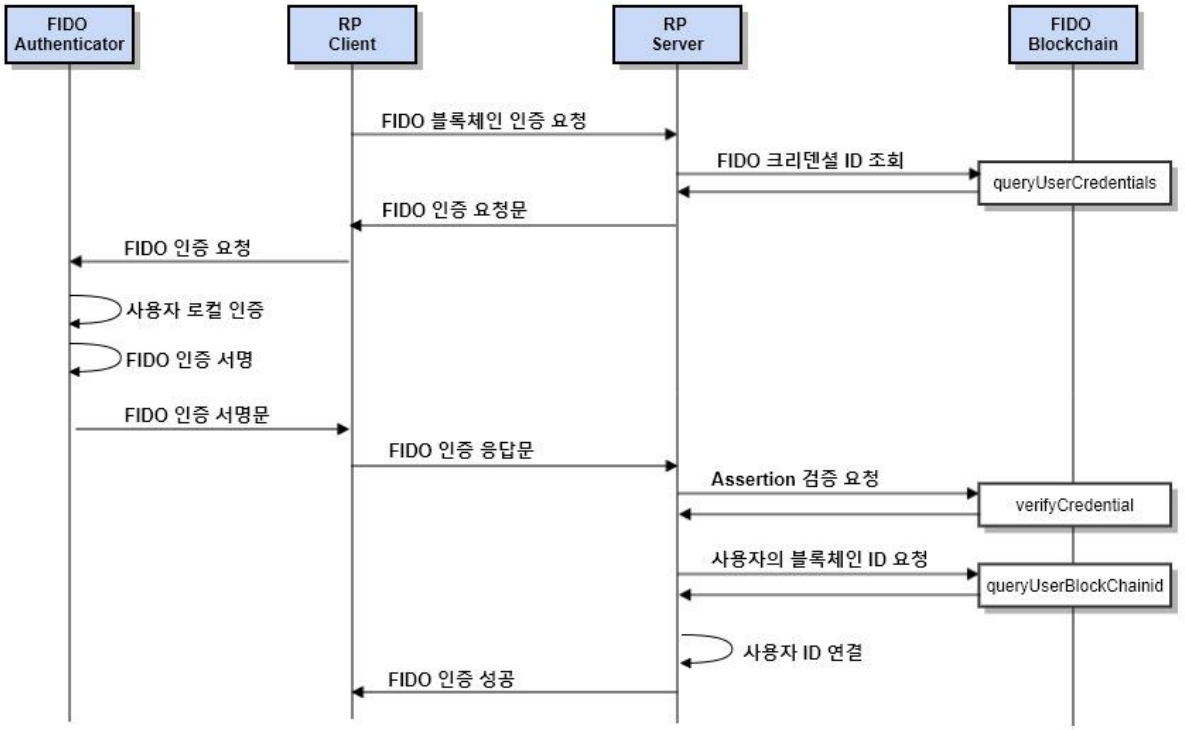
4. FIDO 등록 요청 및 응답
   A. FIDO 인증장치는 FIDO 등록을 위한 사용자 로컬 인증을 수행한다.
   B. 사용자 로컬 인증이 정상이면, FIDO 등록을 위한 사용자 크리덴셜이 포함되어 있는 Attestation 정보를 서버로 전달 한다.
5. FIDO 등록 응답 검증
   A. 스마트 컨트랙트를 이용해서 FIDO 등록 응답인 Attestation 메시지를 검증하고, 검증이 완료되면 블록체인에 사용자의 크리덴셜이 기록된다
   B. 사용자의 크리덴셜은 사용자의 블록체인 ID를 기준으로 기록된다.
6. FIDO 등록 결과 통보

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

블록체인 기반의 FIDO 인증 및 ID 연결

FIDO 인증은 사용자의 FIDO 인증장치가 개인키로 서명한 서명문을 블록체인에 등록된 사용자의 공개키로 검증하는 것이고, FIDO 인증을 통해서 확인 가능한 사용자의 크리덴셜 ID 정보를 이용해서 블록체인에 기 등록되어 있는 사용자의 블록체인 ID 정보를 확인하고 ID를 연결할 수 있다. 본 표준에서는 사용자의 FIDO 인증정보를 크리덴셜으로 표현하며, 크리덴셜 ID는 FIDO 인증정보에 포함되어 있는 사용자의 공개키 식별자 정보이다. 아래 그림은 블록체인 기반의 FIDO 인증 및 ID 연결 과정을 도식화한 것이다.



(부록 Ⅰ-2) 블록체인 기반의 FIDO 인증 및 ID 연결 흐름 [6]

1. FIDO 블록체인 인증 요청
   A. FIDO 인증장치가 탑재 또는 연결되어 있는 디바이스 ID 정보와 사용자의 생년월일, 성별 정보를 RP 서버에 전달한다. 또는 디바이스 ID와 서비스 ID만을 전달할 수 있다.
2. 사용자의 FIDO 크리덴셜 ID 조회
   A. RP 클라이언트로부터 전달 받은 정보를 이용해서 블록체인 ID를 생성한다. 만약 서비스 ID를 전달 받았다면, RP 서버는 서비스 ID로 기 등록 되어 있는

사용자의 생년월일과 성별 정보를 이용해서 블록체인 ID를 생성한다.

B. 스마트 컨트랙트를 이용해서 블록체인에 기록되어 있는 사용자의 FIDO 크리덴셜 ID 정보 조회한다.

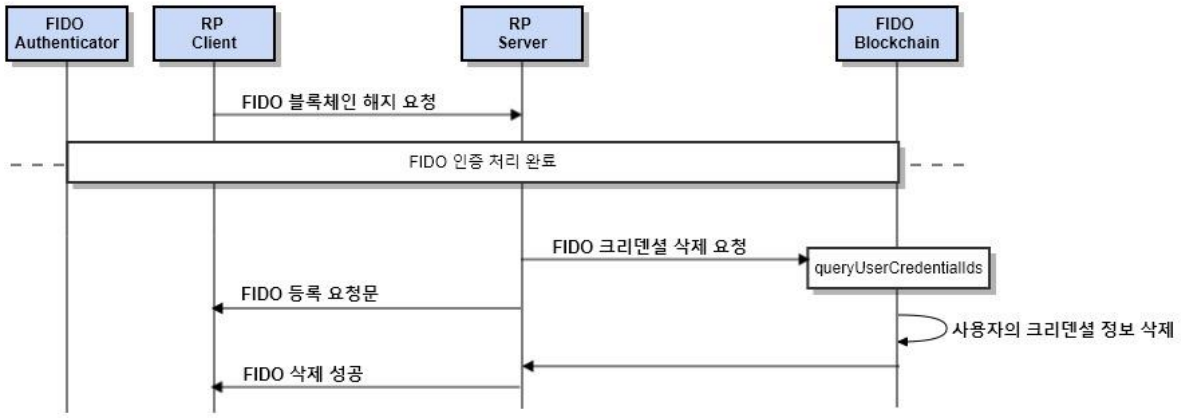
3. FIDO 인증 요청문 생성
   A. 조회된 사용자의 FIDO 크리덴셜 정보 중에서 크리덴셜 ID 정보만을 이용해서 allowed 옵션을 구성하고, FIDO 인증 요청 메시지를 생성한다.
   B. allowed 옵션은 해당 FIDO 크리덴셜 정보와 연관된 FIDO 인증장치에서만 FIDO 인증을 위한 Assertion 정보를 생성할 수 있다.
4. FIDO 인증 요청 및 응답
   A. FIDO 인증장치는 FIDO 인증을 위한 사용자 로컬 인증을 수행하고, 사용자의 크리덴셜을 이용하여 Assertion 정보를 서버로 전달 한다.
5. FIDO 인증 응답 검증 및 ID 연결
   A. 스마트 컨트랙트를 이용해서 FIDO 인증 응답인 Assertion 정보를 검증하고, 검증이 완료되면 블록체인에 사용자의 크리덴셜을 업데이트 한다.
6. 사용자의 블록체인 ID 요청
   A. 스마트 컨트랙트를 이용해서 사용자의 블록체인 ID를 조회한다. 조회를 위해서 필요한 정보는 FIDO 인증을 위해서 사용한 크리덴셜 ID를 이용한다
7. 사용자 ID 연결
   A. 조회한 블록체인 ID와 서비스 ID를 연결하고, 이후 FIDO 인증을 요청할 때에는 블록체인 ID를 이용해서 블록체인에 기록되어 있는 사용자의 FIDO 크리덴셜을 쉽게 조회할 수 있다.
8. FIDO 인증 결과 통보

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

블록체인 기반의 FIDO 해지

FIDO 해지는 블록체인에 기록되어 있는 사용자의 FIDO 인증정보를 삭제하는 것이고, 삭제하려고 하는 FIDO 인증정보에 대한 소유자를 식별하기 위해서 해당 FIDO 인증정보를 통해서 FIDO 인증을 먼저 처리한다. FIDO 인증이 정상적으로 완료되면 블록체인에 기록된 사용자의 FIDO 인증정보를 삭제할 수 있다. 본 표준에서는 사용자의 FIDO 인증정보를 크리덴셜으로 표현하며, 크리덴셜 ID는 FIDO 인증정보에 포함되어 있는 사용자의 공개키 식별자 정보이다. 아래 그림은 블록체인 기반의 FIDO 해지 과정을 도식화 한 것이다.



(부록 Ⅰ-3) 블록체인 기반의 FIDO 해지 흐름 [6]

1. FIDO 블록체인 해지 요청
   A. FIDO 인증장치가 탑재 또는 연결되어 있는 디바이스 ID 정보와 사용자의 생년월일, 성별 정보를 RP 서버에 전달한다. 또는 디바이스 ID와 서비스 ID만을 전달할 수 있다.
2. 사용자의 FIDO 인증 검증
   A. 삭제하려고 하는 사용자의 FIDO 인증정보에 대한 소유자를 검증하는 단계로서 해당 FIDO 크리덴셜에 대한 FIDO 인증 과정이 완료되어야지만 블록체인에 기록되어 있는 사용자의 FIDO 크리덴셜을 삭제할 수 있다.
3. 사용자의 FIDO 인증정보 삭제 요청
   A. 스마트 컨트랙트를 이용해서 사용자의 FIDO 인증정보를 블록체인에서 삭제한다.
4. FIDO 해지 결과 통보

부 록 II-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

II-1.1 지식재산권 확약서(1)

- 출원명: 단말 장치, 서버 장치 및 블록체인을 이용한 FIDO 범용 인증 방법
- 지식재산권자: 한국전자통신연구원
- 출원번호: 10-2018-0080792
- 출원일: 2018년 7월 11일
- 실시조건: 지식재산권을 합리적 조건하에 비차별적으로 실시
- 확약서 접수일: 2018년 7월 5일

부 록 II-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

해당사항 없음

부 록 II-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당사항 없음

부 록 II-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] FIDO Alliance, “What is FIDO?”, https://fidoalliance.org/about/what-is-fido/

[2] FIDO Alliance, “FIDO Metadata Statements”, https://fidoalliance.org/specs/fido-uaf-v1.1-id-20170202/fido-metadatastatement-v1.1-id-20170202.html

[3] MDS web docs, “Same-origin-policy”, https://developer.mozilla.org/en-US/docs/Web/Security/Same-origin_policy

[4] Wikipedia, “Blockchain”, 2017, https://en.wikipedia.org/wiki/Blockchain

[5] TTA 용어사전, “스마트 계약”, http://terms.tta.or.kr/dictionary/dictionaryView.do?word_seq=139368-7

[6] 김석현, 허세영, 조영섭, 조상래, 김수형, “블록체인 기반의 FIDO 범용 인증 시스템”, 전자통신동향분석 33권 1호, 2018.02

[7] TTA, TTAK.KO-12.0292, “신원확인 관리 지침”, 2016.06

부 록 II-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당사항 없음

부 록 II-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	-	-	-	정보보호기술위원회(TC5)