모바일 신분증 - 제1부: 분산 식별자 기반 모바일 운전면허증

이종혁 PG1006(블록체인기반기술) 의장, 세종대학교 정보보호학과 교수
이태양 PG1006(블록체인기반기술) 위원, 세종대학교 정보보호학과 연구원

1. 머리말

민원 신청, 금융 상품 가입, 주류 구입, 렌터카 및 공유킥보드 대여 등 공공, 민간 서비스 이용에 요구되는 것이 공신력 있는 신분증이다. 기존에는 서비스 이용자가 정부에서 발행한 플라스틱 카드 형태의 신분증을 소지하고 서비스 제공자가 육안 식별을 통해 신분증에 있는 증명사진과 신분증 소지자를 대조하여 신원 및 자격을 확인하였다.

기존 신원확인 방식은 분실 및 미소지로 인한 서비스 이용 제한, 용이한 위변조, 불필요한 개인정보 노출 등의 문제가 존재한다. 또한, 온라인에서 활용이 어려워 추가적인 신원확인 수단이 필요하다. 이러한 문제와 디지털 정부혁신을 위한 '디지털 정부혁신 추진계획'에 기반해 모바일 신분증 도입을 위한 노력이 이루어지고 있다.

모바일 신분증은 플라스틱 카드 형태의 신분증과 동일한 법적 효력을 갖는 디지털 형태의 신분증으로, 기존 신분증의 한계들을 해결하였다. 이에 따라, 모바일 신분증과 모바일 신분증 관련 표준의 높은 수요가 기대된다. 따라서 본고에서는 모바일 신분증 중 모바일 운전면허증에 대한 표준을 소개하고자 한다.

2. 모바일 운전면허증 특징

2.1 자기주권 신원증명 (SSI, Self-Sovereign Identity)

운전면허증은 자동차나 원동기장치자전거 운전 자격 확인을 위한 면허 조건, 면허 종류 등의 자격정보와 신분증에서 기본적으로 제공되는 이름, 주민등록번호, 주소지처럼 개인 식별이 가능한 정보까지도 포함한다. 따라서, 운전면허증으로 신원 및 자격을 증명할 때, 증명에 불필요한 정보까지도 노출하게 되어 사생활 및 개인정보가 침해되기도 한다.

이를 해결하기 위해서는 신원 및 자격 검증 시 신분증에 포함된 모든 정보를 제공하는 것이 아니라 검증에 필요한 정보만을 제공할 수 있어야 한다. 이를 위해 자기주권 신원증명 원칙에 기반한 신원증명 개념이 모바일 운전면허증에 적용되었다[1].

2.2 탈중앙화 신원 관리

2.2.1 분산 식별자 (DID, Decentralized Identifier)

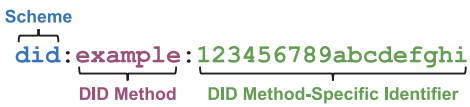
분산 식별자에 대한 표준화를 주도하는 W3C에 따르면 분산 식별자는 중앙화된 등록 기관 없이 식별 대상에 의해 관리되는 식별자로 정의되며, [그림

1]과 같은 구조를 갖는다[2]. 탈중앙화를 위해 분산 식별자는 분산원장 기술 또는 블록체인 기반 환경에서 활용된다. 분산 식별자의 소유권을 증명할 수 있는 공개키, 암호알고리즘 등의 정보는 DID 문서(Document)에 포함되며, 필요시에 DID Method-Specific Identifier를 통해 분산원장 또는 블록체인 기반의 신뢰 저장소로부터 획득할 수 있다[3].

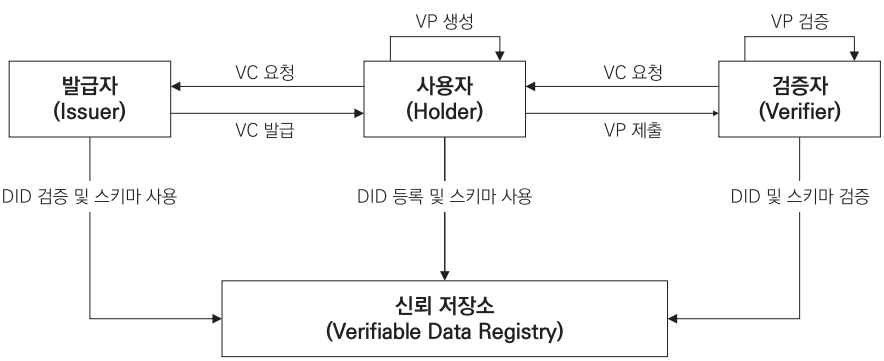
2.2.2 탈중앙/자기주권 신원증명

W3C에서는 분산 식별자 기반 신원증명 서비스 구현을 위해 탈중앙/자기주권 신원증명 모델을 [그림 2]와 같이 정의하였다[4]. 해당 모델은 발급자(Issuer), 사용자(Holder), 검증자(Verifier), 신뢰 저장소(Verifiable Data Registry)로 구성된다. 발급자는 신원증명의 대상인 사용자의 요청에 따라 검증 가능한 자격증명(VC, Verifiable Credential)을 발급하고 자격증명(Credential) 검증에 활용되는 발행자의 공개키와 사용자의 공개키 등의 정보를 신뢰 저장소에 등록한다. 사용자는 발급받은 검증 가능한 자격증명(VC)을 통해 검증자가 요청하는 클레임으로 구성된 검증 가능한 프레젠테이션(VP, Verifiable Presentation)을 생성하고 개인키로 서명하여 검증자에게 제출한다. 검증자는 사용자가 제출한 검증 가능한 프레젠테이션(VP)을 검증하기 위해 발급자와 소유자의 DID 문서 등 필요한 정보들을 신뢰 저장소에서 획득하여 VP를 검증한다.

탈중앙/자기주권 신원증명 모델에서는 사용자의 신원정보 및 자격정보가 암호화되고, 분산원장기술/블록체인 기반 환경에서 분산 식별자의 진위를 실시간으로 검증하기 때문에 신원증명에 사용되는 정보 위조가 불가능하다. 또한, 사용자가 VP를 생성하면서 신원증명에 필요한 정보만을 선택해 검증자에게 제출할 수 있으므로 정보 주체의 주권을 실현할 수 있다[5]. 또한, 기존의 중앙집중형 신원증명 방식과 달리 제3자가 신원증명 과정에 개입하지 않고, 신원정보 활용 이력이 중앙 서버에 저장되지 않는다. 이러한 탈중앙/자기주권 신원증명 모델에 기반한 모바일 운전면허증을 통해 불필요한 개인정보 노출을 최소화하고 정보의 신뢰성 및 보안성이 확보된 신원증명 서비스를 마련할 수 있다[1].



[그림 1] DID 구조



[그림 2] 탈중앙/자기주권 신원증명 모델

2.3 온·오프라인 통합 형태

모바일 운전면허증은 디지털 형태로 구현되기 때문에 스마트폰에서 모바일 운전면허증 앱을 통해 활용할 수 있다. 이에 따라, 온라인에서 로그인과 신원정보 입력이 필요할 때 간편하게 모바일 운전면허증을 활용할 수 있다. 또한, 모바일 운전면허증은 육안 식별이 가능하도록 기존 플라스틱 카드 형태의 운전면허증을 스마트폰 화면에 표출할 수 있고, 재해재난 상황을 고려하여 오프라인 환경에서도 사용할 수 있도록 구현되었다.

3. 분산 식별자 기반 모바일 운전면허증 표준

3.1 표준 개발 목적

'모바일 신분증 - 제1부: 분산 식별자 기반 모바일 운전면허증' 표준은 첫 번째 모바일 신분증 표준으로 모바일 운전면허증 규격에 대해 기술한다. 본 표준에서는 탈중앙/자기주권 신원증명 모델을 기반으로 하는 모바일 운전면허증에서 활용되는 분산 식별자, DID 문서, VC, VP, 분산 식별자 상호 작용 규격을 정의한다.

3.2 표준 요약

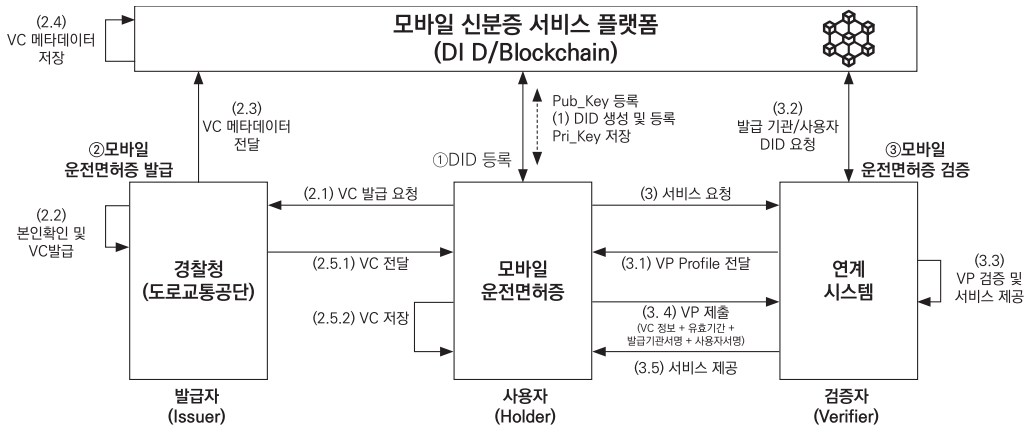
3.2.1 모바일 운전면허증 시스템

모바일 운전면허증 시스템은 기존의 중앙집중식 운전면허증 시스템을 대체하기 위한 것으로, [그림 3]과 같이 분산 식별자에 기반한 탈중앙화된 시스템이다[6]. 모바일 운전면허증 시스템에서 참여자들은 분산 식별자를 통해 해당 시스템에 등록되어야 한다. 각 참여자는 분산 식별자를 생성하고 DID 문서를 블록체인에 등록함으로서 모바일 운전면허증 시스템에 참여할 수 있다.

모바일 운전면허증 시스템은 안정적인 서비스 제공을 위해 재전송 공격에 대응하고, 부인 방지, 통신 보안, 합의 알고리즘을 지원할 수 있어야 한다. 또한, 개인을 식별할 수 있는 정보는 블록체인에 저장되지 않도록 하여 개인정보를 보호할 수 있어야 한다.

3.2.2 분산 식별자 규격

모바일 운전면허증 시스템 참여자에는 발급자, 사용자, 검증자뿐만 아니라 모바일 운전면허증 발급기관 서버(Issuer Authority), 모바일 신분증 서버



[그림 3] 모바일 운전면허증 시스템

<표 1> 분산 식별자 규격 및 Method

분산 식별자 규격	kr-did = "did:kr:mobileid:kr-identifier"
분산 식별자 Method	국가 모바일 신분증을 식별하기 위한 DID Method의 문자열은 "kr"이고, 모바일 신분증은 sub-name 문자열로 "mobileid"가 추가된 "kr:mobileid"이다. 모바일 운전면허증도 동일하게 사용한다.
모바일 운전면허증 분산 식별자 예제	did:kr:mobileid:1234567890

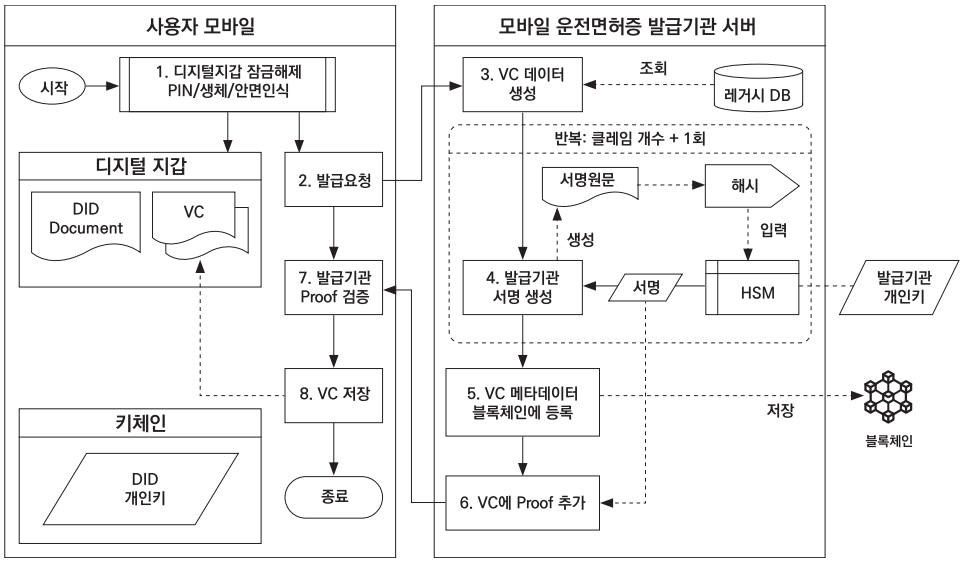
(Trust Agent), 검증 서버(Verifier Agent), 중계 서버(Proxy Agent)도 포함될 수 있다. 이들은 모바일 운전면허증 시스템에서 분산 식별자를 통해 고유하게 식별된다. 모바일 운전면허증 시스템에서의 분산 식별자는 <표 2>와 같이 국가 모바일 신분증을 식별하기 위한 DID Method를 동일하게 사용한다[6].

모바일 운전면허증 시스템 참여자들에 대한 정보 중 공개키, 분산 식별자가 인증에 사용될 수 있는 방법, 상호작용을 위한 채널 간 암호화 방법, 기타 확장 가능한 정보 등은 DID 문서에 포함되어 블록체인에 저장된다. DID 문서는 생성(Create)-읽기(Read)-갱신(Update)-폐기(Delete) 주기를 가지며, CRUD 작업은 RESTful API를 통해 지원된다.

3.2.3 자격증명 규격 및 절차

모바일 운전면허증 시스템에서 VC는 자격증명 주체, 발급기관, 주체에 대한 클레임을 포함한다. VC는 Non-ZKP VC와 ZKP VC 2가지 형태로 활용될 수 있다. ZKP VC는 영지식 증명(ZKP, Zero-Knowledge Proof) 기술이 적용된 것으로, 증명하고자 하는 정보를 직접적으로 공개하지 않고 검증하고자 하는 자격을 갖추었는지 확인할 수 있도록 하여 개인정보를 보호할 수 있다. VC를 발급하는 절차는 [그림 4]와 같을 수 있다[6].

검증기관은 사용자의 신원 및 자격을 검증하기 위해 사용자에게 VP 제출을 요청할 때 제출 정보를 명시한 VP Profile을 동적으로 생성할 수 있다. VP도



[그림 4] VC 발급절차

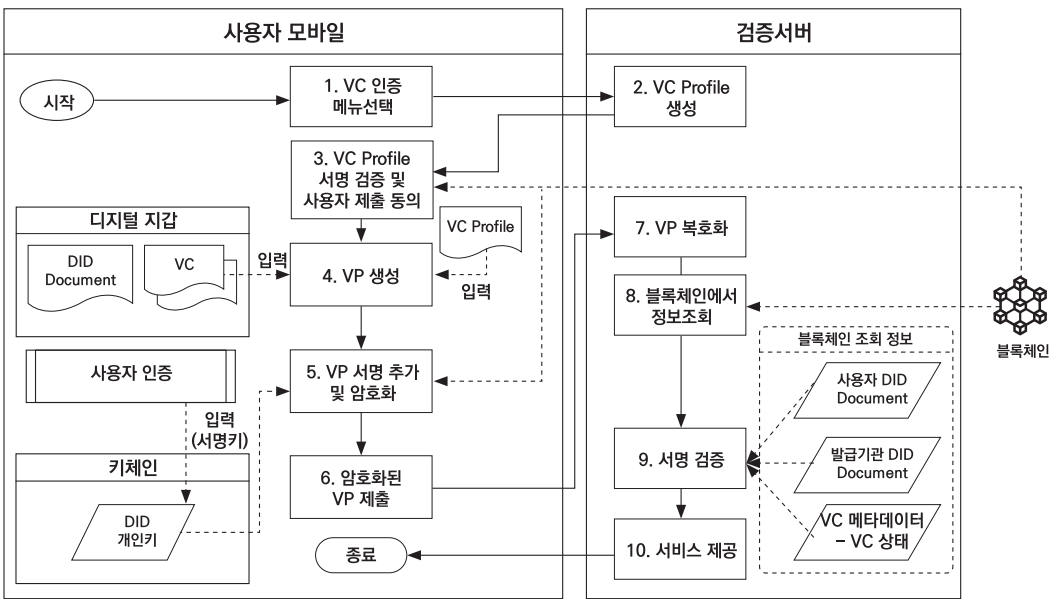
Non-ZKP VP와 ZKP VP 2가지 형태로 활용될 수 있기 때문에, VP Profile도 Non-ZKP VP Profile과 ZKP VP Profile 2가지 형태로 생성되어야 한다. 이때, Non-ZKP VP의 경우, 사용자의 개인정보가 제출되기 때문에 사용자에게 요청할 제출 정보에 대해 모바일 운전면허증 시스템의 운영협의체로부터 승인받아야 한다. 이를 위해 VP Profile Document가 활용되며, 운영협의체로부터 승인받은 VP Profile Document는 블록체인에 등록해 두었다가 Non-ZKP VP Profile 생성 시 활용된다. VP 발급절차는 [그림 5]와 같을 수 있다[6].

3.2.4 상호 작용 규격

모바일 운전면허증은 다양한 환경에서 활용 가능하도록 QR 코드 활용 인터페이스(QR-MPM, QR-CPM), 모바일 운전면허증 앱 활용 인터페이스(App2App), PUSH 메시지, 블루투스(BLE+QR) 활용 인터페이스 등 다양한 인터페이스를 지원할 수 있다. 또한, 전송방식도 검증기관 서버에 VP를 직접 제출하는 방식(direct), 모바일 운전면허증 앱을 통해 암호화된 VP를 검증기관 서버에 전달하는 방식(indirect), 검증기관 서버와의 통신 환경이 불가하여 중계 서버를 이용하여 통신하는 방식(proxy) 지원이 가능하다. 모바일 운전면허증은 인터페이스와 전송방식에 따라 메시지 규격과 보안 처리 방식이 다를 수 있다[6].

4. 맺음말

기존 플라스틱 카드 형태 신분증의 불편함, 개인정보 보호 의식의 개선, 데이터 주권 개념의 부상 등과 맞물려 편의성, 신뢰성, 보안성 측면에서 향상된 모바일 운전면허증은 디지털 시대에 사는 우리에게 다양한 신원증명 서비스를 제공하는 주요한 매체가 될 것이다. 또한, 정부에서는 디지털 정부 혁신을 위해 모바일 신분증 확대에 적극적으로 나서고 있어 모바일



[그림 5] VP 발급절차

운전면허증에 기반한 대국민 서비스 확산이 더욱 촉진될 것이다.

현재 우리나라의 모바일 신분증은 신원확인이라는 본래의 목적에만 머물러 있는 단계이다. 우리나라와 비슷하게 유럽연합에서도 '유럽연합 전자신원확인 및 신뢰서비스에 관한 규정 2.0(eIDAS 2.0, electronic Identification, Authentication and Trust Services 2.0)'을 고려하여 디지털 신원지갑 기반의 신원확인 생태계를 마련하려는 노력이 이루어지고 있다. 유럽연합의 신분증은 전자지갑에 공공기관에서 발행한 신분증뿐만 아니라 민간에서 발행하는 증명서도 탑재 가능하고 개인뿐만 아니라 법인에게도 모바일 신분증을 발행할 수 있는 형태로 사용되고 있다. 이에 따라, 우리나라 모바일 신분증도 eIDAS 2.0의 요건을 준수하면서 모바일 신분증뿐만 아니라 여러 가지 증명서를 담는 형태로 고도화된 신원확인 수단의 마련이 필요한 실정이다[7].

본고에서 소개한 표준은 모바일 운전면허증의 분산 식별자 규격, 자격증명 규격, 상호작용 규격을 정의하고 있으며, 신원증명 서비스의 혁신과 범국가적 모바일 운전면허증 생태계 마련을 위한 기반을 마련했다는 데에 의미가 있다. 또한, 고도화된 신원확인 수단 마련을 위한 기술개발 및 표준안 마련에 널리 활용될 수 있으리라 기대된다.

※ 본 연구는 2023년도 정부(개인정보보호위원회)의 재원으로 한국인터넷진흥원의 지원을 받아 수행된 연구임 (No.1781000011, 블록체인 환경에서의 개인정보보호 표준개발)

참고문헌

[1] 양희선, 이강효, 이종혁, '블록체인 모바일 운전면허증 표준 소개', 전자공학회지, pp. 35-51, 2020년
[2] W3C, Decentralized Identifiers (DIDs) v1.0, 2022년 7월
[3] 김수형, '탈중앙화 신원증명 기술 동향', TTA 저널, vol. 203, pp. 53-60, 2022년 9월/10월
[4] W3C, Verifiable Credential Data Model v2.0, 2024년 1월
[5] 오혜진, '내 정보의 주권은 나에게, 차세대 신원 증명 기술 DID', TTA 저널, vol. 192, pp. 132-133, 2020년 11/12월
[6] TTAK.KO-10.1502-Part1, '모바일 신분증 - 제1부: 분산 식별자 기반 모바일 운전면허증', 2023년 12월
[7] 이종혁, '유럽 디지털 신원지갑의 출현과 우리 금융권에 미치게 될 영향', 전자금융과 금융보안, 제34호, pp.41-54, 2023년 11월

주요 용어 풀이

- **W3C**: 민간 기업 등 회원사가 협력하여 웹 표준을 개발하는 국제 사실표준화기구
- **CRUD**: 생성(Create), 읽기(Read), 갱신(Update), 폐기(Delete)
- **VP Profile**: 서비스 제공자가 서비스를 제공하기 위해 VP Profile Document를 기반으로 서비스 제공자의 증명값과 함께 동적 생성하여 사용자에게 요청하는 제출정보 목록
- **VP Profile Document**: 서비스 제공자가 서비스 제공을 위해 사용자에게 요청하는 제출정보 목록으로 블록체인에 등록하여 VC Profile 생성 시 사용되는 정보