통합 디지털 지갑 구축 및 상호 운용 시 고려사항

서울외국어대학원대학교 박근덕 교수

디지털 지갑 서비스 현황

통합 디지털 지갑(Universal digital wallet)은 시장에서 통용되는 용어로써 추후 표준화된 용어로 정의될 수 있으나, 통합 디지털 지갑과 TTA정보통신용어사전에 정의된 디지털 지갑(Digital wallet)의 의미는 유사하다고 볼 수 있다.

※ 디지털 지갑(Digital wallet)은 디지털 형태로 보관되는 금융 자산이나 신분 증명 등의 각종 정보를 관리하고 금융 거래, 결제, 증명 등을 처리하는 소프트웨어를 의미한다. (출처: TTA정보통신용어사전)

국내 디지털 지갑 서비스

삼성월렛은 삼성전자에서 제공하는 통합 디지털 지갑 서비스로써, 간편 결제, 신분증, 멤버십, 교통카드 등을 제공한다.

쏠지갑은 신한은행에서 제공하는 디지털 지갑 서비스로써, 간편 결제, 포인트, NFT 거래, 신분증(주민등록증), 증명서 등을 제공한다.

카카오(네이버)페이 지갑은 카카오(네이버)에서 제공하는 통합 디지털 지갑 서비스로써, 간편 결제, 교통카드, 멤버십, 쿠폰, 증명서 등을 제공한다.

원더월렛은 우리은행에서 제공하는 디지털 지갑 서비스로써, 국민비서, 전자문서, 자격증명, NFT(Non-fungible token, 대체불가능토큰) 거래 등을 제공한다.

옴니원은 라온시큐어에서 제공하는 DID(Decentralized identity, 분산신원증명) 기반 신원 지갑 서비스로써, 신분증(운전면허증, 주민등록증), 학생증, NFT 거래, 디지털 배지 등을 제공한다.

클립은 안랩블록체인컴퍼니에서 제공하는 디지털 자산 지갑 서비스로써, 가상 자산(이더리움 등) 거래, NFT 거래 등을 제공한다.

국외 디지털 지갑 서비스

구글월렛은 구글(Google)에서 제공하는 통합 디지털 지갑 서비스로써, 간편 결제, 선물용 카드, 비행기 탑승권, 공연 및 영화 티켓 등을 제공한다.

애플월렛은 애플(Apple)에서 제공하는 통합 디지털 지갑 서비스로써, 간편 결제, 교통 카드, 비행기 탑승권, 공연 및 영화 티켓, 자동차 키 등을 제공한다.

EUDI월렛은 EC(유럽 위원회)에서 EU(유럽연합) 시민에게 제공하는 통합 디지털 신원 지갑 서비스로써, 신분증(운전면허증), 비자 및 여권, 유럽 건강 보험 카드, 간편 결제, 교육 증명서, 비행기 탑승권 등을 제공한다.

메타마스크은 컨센시스(Consensys)에서 제공하는 디지털 자산 지갑 서비스로써, 가상자산(비트코인 등) 거래, NFT 거래 등을 제공한다.

국내외 디지털 지갑 관련 표준화 현황

ITU-T SG17(Security), ISO/IEC JTC 1/SC 27/WG 5(Identity management and privacy technologies), ISO/TC 307/JWG 4 (Security, privacy and identity for Blockchain and DLT), TTA PG502(개인정보보호/ID관리, 블록체인 보안 프로젝트그룹) 등 국내외 표준화 기구에서 추진하고 있는 디지털 지갑 관련 표준화 현황은 아래의 표와 같다.

ISO/IEC JTC 1/SC 17/AG 3(Digital identity wallets)에서 디지털 신원 지갑에 관한 표준화 연구를 추진하고 있다.

ITU-T OpenWallet Forum은 다목적 및 글로벌 상호 운용이 가능한 디지털 지갑을 개발 및 배포하면서 글로벌 다중 이해관계자 간의 협력을 강화하기 위하여 활동하고 있다.

OpenWallet Foundation(OWF)은 발행자, 지갑 제공자 및 신뢰 당사자가 이용자의 선택, 정보보호 및 개인정보 보호를 구현하는 디지털 지갑 기술에 관한 모범 사례를 구축하기 위하여 활동하고 있다.

아래의 표에서 보는 바와 같이 디지털 지갑에 대한 국내외 표준화는 초기 단계에 있으나, 그중에 디지털 신원 지갑(Digital identity wallet)에 대한 표준화는 활발히 추진 중이다.

※ 신원 지갑은 사용자가 자신의 개인 키들을 저장함으로써 주로 식별자와 크리덴셜들을 보유하도록 하는 응용이다. (출처: TTA정보통신용어사전)

디지털 지갑 관련 표준화 현황

표준화기구	표준 번호 및 제목	비고
ITU-T SG17	**ITU-T TR.dw-lasf**, Technical report: A landscape analysis and security features for a digital wallet	개발 중 (2025-04), 한국 에디터
	ITU-T X.srdidm, Security requirements for decentralized identity management systems using distributed ledger technology	개발 중 (2025-12), 한국 에디터
	ITU-T X.sfdiw, Security framework of digital identity wallet for decentralized identity model	개발 중 (2026-09), 한국 에디터
ISO/IEC JTC 1 SC 27/WG 5	**ISO/PWI 25863**, Exploration of security and privacy characteristics for digital identity wallets managing digital credentials	개발 중, 한국 코에디터
ISO/TC 307/JWG 4	**ISO/WD 23042**, Reference architecture for DLT-based decentralized identity systems	개발 중, 한국 코에디터
TTA PG502	**TTAR-12.0053**, 유럽 디지털 신원 지갑 아키텍처와 참조구조 프레임워크(기술보고서)	제정(2023-10)
	TTAK.KO-12.0412, 감염병 예방을 위한 분산ID 기반 디지털 증명서 시스템 보안 요구사항	제정(2024-12)

출처: ITU-T, ISO/IEC JTC 1, ISO, TTA

※ PWI(Preliminary work item)은 신규 표준화 작업 항목으로 제안하기 위한 초기 연구 단계의 작업 항목으로써, 통상적으로 타 표준과의 갭분석(Gap analysis)을 통하여 표준의 제목, 범위(Scope), 구조(Structure) 등을 정한다.

통합 디지털 지갑의 필요성 및 구축 방안

이용자의 편리성 제고

신분증, 자격 증명서, 공공 전자문서, 간편 결제, 교통카드, 블록체인 기반 가상 자산 및 디지털 자산 거래 등 다양한 서비스별 디지털 지갑을 각각 설치 및 운용하는 이용자의 불편함을 최소화한다.

이용자의 개인정보 보호 강화

다양한 서비스별 디지털 지갑을 각각 설치 및 운용하기 위하여 다수의 지갑 제공자에게 반복적으로 이용자의 개인정보를 제공하는 것을 지양한다.

시스템 구축 시 고려 사항

<기술적 측면>

이용자 식별 및 인증을 위한 생체인증(예: FIDO), 분산신원증명(DID), 일회용 인증(예: 대역 외 OTP) 등 아이디/패스워드 기반의 인증보다 안전한 인증 수단을 제공한다.

이용자의 개인정보 및 중요정보(예: 금융정보, 신원정보, 의료정보 등)를 보호하기 위한 안전한 암호화 알고리즘 및 통신 프로토콜을 활용한다.

이용자의 단말기(예: 스마트폰 등) 내 타 애플리케이션이 통합 디지털 지갑으로 무단 접근하는 것을 차단한다.

이용자의 단말기 내 타 애플리케이션과 통합 디지털 지갑 간의 서비스 연동 및 확장을 위하여 공통의 인터페이스 (예: API)를 제공한다.

통합 디지털 지갑 이용 내역을 블록체인에 저장 및 관리하여 위·변조를 방지하고, 만일의 보안 사고 발생 시 역추적 기능을 제공한다.

다수의 이용자 단말기(예: 스마트폰, 태블릿PC, 랩톱 등)에서 통합 디지털 지갑을 이용할 수 있도록 지갑 복사, 지갑 이전(Migration) 기능을 제공한다.

〈서비스 측면〉

정부24 등 공공 서비스와 통합 디지털 지갑을 연동하여 각종 전자문서, 전자증명서, 모바일 신분증 등의 서비스를 제공한다.

금융(예: 은행, 카드, 보험, 증권, 가상자산사업자 등), 의료(예: 병원, 보건소 등), 교육(초중고, 대학, 직업학교 등), 교통(예: 버스, 철도, 선박, 항공 등) 등 다양한 산업 분야의 서비스와 통합 디지털 지갑을 연동하여 간편 결제, 송금, 가상 자산 및 디지털 자산 거래, 건강 증명서, 디지털 배지, 대중교통 카드, 탑승권 등의 서비스를 제공한다.

〈법제도적 측면〉

정보보호 및 개인정보 보호, 자금세탁 및 불법자금조성 방지, 디지털 신원, 가상 자산 및 디지털 자산, 블록체인 기술 및 산업 활성화 등 관련 법령 제·개정, 기존 제도 보완 및 신규 제도 마련 등을 통한 통합 디지털 지갑의 이용자 보호 및 시장 규모를 확대한다.

통합 디지털 지갑 간 상호운용성을 위한 기술적 고려사항

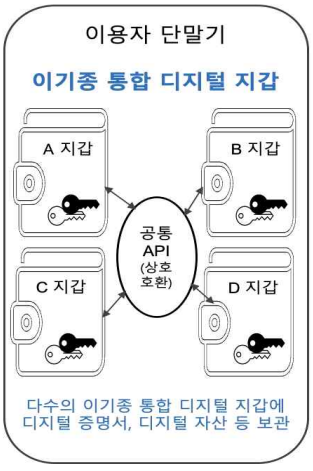
공통의 인터페이스

이용자 단말기 내에서 운용하고 있는 이기종 통합 디지털 지갑을 상호 연동하기 위한 공통의 인터페이스(예: API)를 식별 및 구현한다.

디지털 지갑 및 증명서의 생명주기 기반 공통의 인터페이스는 다음과 같은 기능 요구사항을 포함할 수 있고, 통합 디지털 지갑 개발자에게 권고할 수 있는 국내외 표준화를 고려한다.

- 식별 및 인증(예: 타 지갑에 대한 접근 권한 획득)
- 정보 조회(예: 타 지갑의 디지털 증명서, 가상 자산 및 디지털 자산 관련 현황 획득)
- 정보 전송(예: 타 지갑의 디지털 증명서, 가상 자산 및 디지털 자산 관련 세부 정보 획득)
- 정보 이용(예: 타 지갑의 디지털 증명서, 가상 자산 및 디지털 자산 관련 이용 요청 및 실행)

통합 디지털 지갑 연동을 위한 공통의 인터페이스

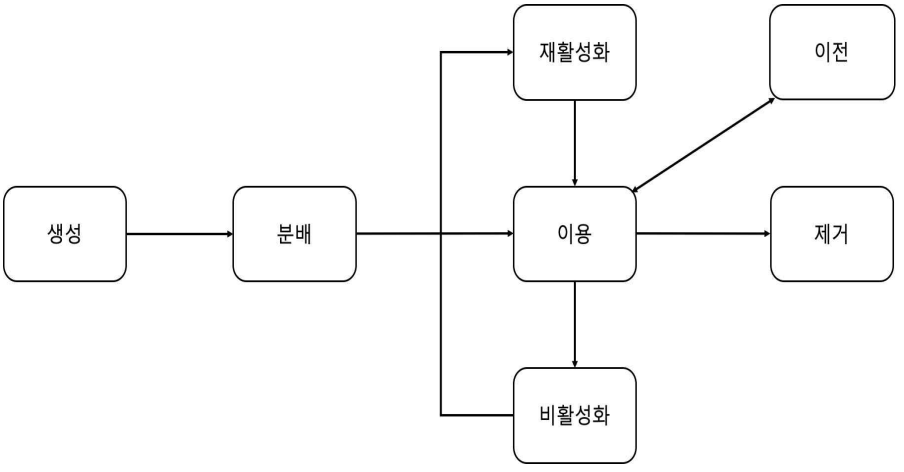


출처: 서울외국어대학원대학교

디지털 지갑의 생명주기 관리

디지털 지갑 서비스는 디지털 지갑의 생명주기(생성에서 제거까지의 전 단계)를 내포하고 있으므로, 이기종 디지털 지갑 간 상호운용성을 구현하기 위하여 생명주기 관리 및 표준화가 필요하다.

디지털 지갑의 생명주기 관리 모델



출처: 서울외국어대학원대학교

생성(Generation) 단계는 개발자는 법적 요구사항, 기능 요구사항, 보안 요구사항 등을 고려하여 디지털 지갑을 개발하고, 해당 요구사항이 적절히 구현되었는지 시험한다.

배포(Distribution) 단계는 개발자는 생성된 디지털 지갑을 홈페이지 또는 온라인 스토어 등에 등록하고, 이용자가 디지털 지갑을 다운로드 시 위·변조되지 않도록 해야 한다.

이용(Usage) 단계는 이용자 단말기에 디지털 지갑을 설치하고, 이용자의 디지털 증명서, 가상 자산 및 디지털 자산 등의 소유권을 증명하기 위한 고유한 개인 키·공개키 쌍을 생성할 수 있다. 디지털

지갑은 이용자를 식별 및 인증해야 하고, 디지털 지갑의 이용 내역은 안전하게 저장 및 관리되어야 하며, 이용자 단말기 내 타 애플리케이션이 디지털 지갑에 무단으로 접근하는 것을 방지해야 한다.

이전(Migration) 단계는 이용자 단말기에 설치된 디지털 지갑을 이용자의 다른 단말기로 이동함. 디지털 지갑 이동 시 해당 지갑에 저장된 모든 데이터가 위·변조되지 않도록 해야 한다.

비활성화(Deactivation) 단계는 이용자는 일정 기간 동안 디지털 지갑을 더 이상 이용할 수 없도록 비활성화하고, 비활성화된 디지털 지갑에 저장된 모든 데이터에 대한 접근은 차단되어야 한다.

재활성화(Reactivation) 단계는 이용자는 비활성화된 디지털 지갑을 다시 이용할 수 있도록 재활성화한다.

제거(Removal) 단계는 이용자 단말기에 설치된 디지털 지갑을 제거하고, 디지털 지갑에 저장된 모든 데이터는 복구되지 않도록 삭제되어야 한다.

※ 또한 이기종 디지털 지갑 간 상호운용성을 구현하기 위하여 디지털 증명서의 생명주기(발행에서 폐기까지의 전 단계) 관리 및 표준화가 필요하다.