J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

전자지갑 유형 및 보안 특성 분석

Analysis of Electronic Wallet Types and Security Features

김 문 성[1] 임 형 진[2*]
Moonseong Kim Hyung-Jin Lim

요 약

디지털 자산의 관리와 보호는 사용자 개인정보와 재산을 안전하게 지키기 위해 필수적이다. 특히 블록체인 기술과 암호화폐의 발전은 디지털 자산의 위험을 증가시켰으며, 이에 따라 전자지갑의 활용이 증가하고 있다. 그러나 전자지갑의 표준화된 정의나 구현이 부족하여 정체성이 불명확한 상황이다. 본 논문은 전자지갑의 주요 유형인 디지털 ID 지갑, 디지털 결제 지갑, 암호화폐 지갑을 분류하고, 각 유형의 보안 특성을 비교 분석한다. 디지털 ID 지갑은 신원 정보를 안전하게 관리하며, 디지털 결제 지갑은 결제 정보를 저장하고 금융 서비스를 지원한다. 암호화폐 지갑은 디지털 화폐의 거래와 저장을 담당하며, 보안 위협에 대비한 개인키 관리가 중요한 역할을 한다. 본 연구는 전자지갑의 보안성을 향상시키기 위한 기술적 요구사항을 제시하고, 디지털 자산의 안전한 관리를 위한 방향성을 제시한다.

☞ 주제어 : 디지털 지갑, 디지털 ID 지갑, 디지털 결제 지갑, 디지털 자산, 보안

ABSTRACT

The management and protection of digital assets are essential for safeguarding users' personal information and wealth. In particular, the development of blockchain technology and cryptocurrencies has increased the risks associated with digital assets, leading to a rise in the use of digital wallets. However, the lack of standardized definitions and implementations of digital wallets has resulted in unclear identities. This paper classifies the main types of digital wallets: Digital ID wallets, Digital payment wallets, and Cryptocurrency wallets, and compares their security characteristics. Digital ID wallets securely manage identity information, digital payment wallets store payment information and support financial services, and cryptocurrency wallets are responsible for the transaction and storage of digital currencies, with personal key management playing a crucial role in mitigating security threats. This study presents the technical requirements for enhancing the security of digital wallets and offers directions for the safe management of digital assets.

☞ keyword : Digital wallets, Digital ID wallets, Digital payment wallets, Digital assets, security

1. 서 론

디지털 자산의 효율적인 관리와 보호는 사용자 재산과 개인정보를 안전하게 지키는 데 중요하다. 특히, 블록체인 기술과 암호화폐 시장의 확대는 테라-루나 사태 등과 같은 사건으로 디지털 자산의 위험을 증가시키고 있다 [1]. 다양한 디지털 자산의 유통으로 전자지갑의 활용이 증가하고 있지만, 표준화된 용어와 구현이 없어 정체성이 불명확하다. 디지털 자산은 경제적 가치를 지닌 모든 전자적 데이터를 포함하며, 최근에는 분산원장기술로 생성된 암호화폐나 토큰도 포함된다 [2].

전자지갑은 온·오프라인 금융거래, 디지털 예술품 및 신원 증명 관리 등에 활용되며, 비트코인 같은 암호화폐를 저장하는 암호화폐 지갑도 포함된다. 전자지갑은 디지털 자산을 안전하게 보관하고 관리하는 도구로, 암호화폐, 결제정보, 신원 정보 등을 저장하고 관리한다. 암호화폐 지갑은 블록체인의 접근제어와 거래를 수행하는 새로운 형태의 전자지갑이다 [3]. 본 논문에서는 전자지갑의 주요 유형을 분류하고, 각 유형의 보안 특성을 비교 분석하여 전자지갑의 기술적 동향을 파악한다.

본 논문은 다음과 같이 구성된다. 2장에서는 관련 연구에 대해 소개하고, 3장에서는 전자지갑의 유형을 설명한다. 그리고 4장에서는 각 보안 특성을 간단히 분석하며, 마지막으로 5장에서 결론을 맺는다.

1 Dept. of IT Convergence Software, Seoul Theological University, Bucheon, 14754, Korea.
2 Financial Security Institute, Seoul, 07332, Korea.
* Corresponding author (hjlim@fsec.or.kr)
[Received 30 November 2024, Reviewed 4 December 2024, Accepted 10 December 2024]
☆ This work was supported by the Seoul Theological University Research Fund of 2024.

2. 관련 연구

전자지갑은 1990년대 초반에 처음 등장했으며, 디지털 결제와 자산 관리의 필요성에 따라 발전해왔다. 초기에는 간단한 온라인 결제 수단이었지만, 인터넷과 모바일 기술의 발전으로 다양한 기능을 제공하는 복합적인 플랫폼으로 진화했다. 전자지갑은 ID 관리 및 결제 영역에서 다양한 서비스를 지원하는 보조 수단으로 역할을 해왔다. 논문 [4]는 전자지갑 결제 방법은 현금과 신용카드와 같은 전통적인 결제 방법과 비교 분석하였다. 또한, 온라인, 모바일, 데스크탑 등의 사용자 단말기 형태에 따른 전자지갑의 발전과 암호화폐 지갑으로의 전환을 소개하며, 디지털 자산 보호를 위한 신원정보의 안전한 관리 중요성을 강조하였다.

2010년대에는 스마트폰의 확산과 함께 신용카드 결제를 위한 안전한 모바일 전자지갑 구현에 대한 연구가 진행되었다. 논문 [5]는 주요 IT 사업자들이 주도하는 모바일 결제 서비스 구조와 보안 특성을 비교 분석하였다. 최근에는 모바일 결제와 분산형 인증 기술 기반의 전자지갑 서비스가 등장했으며, 사용자 기기 설치형과 제3자 위임형으로 분류하여 보안 위협과 요구사항을 분석하는 연구도 이루어지고 있다 [6].

비트코인을 중심으로 암호화폐 시장이 확대되면서 전자지갑 및 보안 강화의 필요성이 대두되고 있다. 다양한 상용 전자지갑 제품들이 암호화폐 타입, 키 관리 방식, 플랫폼 유형, 키 복구 방식 등에 따라 비교 분석되고 있다. 전자지갑은 사용자의 키 관리 여부에 따라 사용자 관리 지갑, 거래소 관리 지갑, 전문 관리 지갑으로 분류되며, 인터넷 연결성에 따라 핫월렛, 콜드월렛, 웜월렛으로 나뉜다 [7-8]. 전자지갑은 암호화폐, NFT, ID관리를 지원하며, 온·오프라인의 다양한 서비스를 제공하는 포털로 발전하고 있다.

최근 전자지갑은 간편결제, 가상자산, 법정 화폐, 신원증명 등 다양한 분야에서 사용되며, 각 분야별 구현 방식과 보안 요구사항이 비교되고 있다. 기존 연구는 주로 ID 관리와 결제 서비스 관점에서 전자지갑을 다뤘으며, 암호화폐 관련 연구는 안전한 키 관리에 집중하고 있다. 그러나 대부분의 연구는 특정 시기에 사용된 전자지갑의 보안 및 기술 요구사항에 한정되어 있으며, 전자지갑이 디지털 자산을 관리하는 수단으로 발전함에 따라 기술적·보안적 요구사항을 식별하는 것이 중요하다.

3. 전자지갑의 유형

디지털 ID 지갑은 사용자의 신원 정보를 디지털 형태로 저장하고 관리하는 전자지갑으로, 신원 검증 및 인증을 간편하게 하며 여러 플랫폼 간 신원정보 통합을 지원한다. 이를 통해 사용자는 다양한 서비스에 접근하고 개인 정보 보안을 강화할 수 있다. 디지털 ID 지갑은 암호화 기술, 멀티 팩터 인증 등을 결합하여 신원정보 보호에 중요한 역할을 하며, 금융 및 공공기관과 연계하여 온라인 인증, 정부 서비스 접근, 결제 및 송금 등의 기능을 제공한다. 또한, 신원 정보는 공개 정보부터 주민등록번호, 신용카드 번호 등 다양한 정보를 포함하고, 사용자 중심의 신원 정보 관리 모델로 발전하고 있다 [9-11].

디지털 ID 관리 시스템은 인터넷 발전에 따라 사용자 신원 정보의 관리 방식이 변화해 왔다. 초기에는 클라이언트-서버 모델을 기반으로 하여, 사용자는 ID 식별자와 비밀 정보를 통해 시스템에 접근했다. 시간이 지나면서 디지털 ID 관리 구조는 서비스 제공자에서 사용자 중심으로 변화했으며, 개인이 자신의 신원 정보를 직접 관리하는 방식으로 발전했다. 스마트폰 보급과 함께 디지털 ID 지갑이 등장하였고, 이를 통해 사용자는 여러 ID 식별자를 안전하게 관리할 수 있게 되었다. 최근에는 블록체인 기반의 분산형 ID 지갑이 등장하여, 중앙 서버 없이 사용자 정보가 분산원장에 저장되고 개인정보 보호와 데이터 소유권을 강조하는 방향으로 발전하고 있다. 이를 활용한 서비스로는 모바일 운전면허증, 전자증명서 등이 있으며, EU는 eIDS 규격을 제정하여 디지털 신분증 서비스를 확산하고 있다 [12].

디지털 결제 지갑은 온·오프라인 결제 및 금융 정보를 관리하는 소프트웨어나 웹 서비스로, 주로 신용카드와 같은 금융 정보를 저장하고 제어하는 기능을 제공한다. 특히, 휴대폰 기반의 디지털 결제 지갑은 2000년대 일본의 근거리 무선 결제 서비스에서 발전하였으며, NFC 기술을 통해 모바일 기기와 결제 단말기의 터치로 결제가 가능하다. 이 지갑은 은행 계좌, 신용카드 정보, 전자 머니 등을 저장하며, 온라인 결제, 오프라인 결제(NFC·QR 코드), 송금, 리워드 프로그램, 개인 금융 관리 등 다양한 부가서비스를 제공한다. 대표적인 디지털 결제 지갑으로는 알리페이, 애플 페이, 삼성 페이 등이 있으며, 결제 중심의 서비스에 멤버십카드, 티켓 저장 등 비결제적 기능이 결합된 형태로 제공된다 [13-14].

표 1에서 설명한 바와 같이 디지털 결제 지갑은 독립적인 서비스라기보다는 결제 서비스를 중심으로 멤버십

카드, 티켓 저장 등 비결제 기능을 필요에 따라 조합하여 제공하는 형태에 가깝다. 모바일 지갑 서비스는 모바일이라는 단일 접근 매체에 신용카드, 쿠폰, 신분증 등을 결합하여 일상적으로 사용하는 다양한 기능을 복합적으로 제공한다.

(표 1) 디지털 결제 지갑 서비스 [13]
(Table 1) Digital Payment Wallet Services [13]

분야	사례
결제 서비스	• 모바일 카드 등으로 오프라인 가맹점 결제 • 모바일 P2P, P2B, B2B 이체
상거래 서비스	• 쿠폰, 할인 혜택등 각종 로열티 서비스 • 각종 티켓, 교환권 • 위치기반 서비스
뱅킹 서비스	• 요금납부, 연금 입출금 • 계좌정보, 거래 내역 조회 • 투자, 자산관리
ID 서비스	• 각종 신분증 • 전자서명 (로그인을 통한 접근제한 등)

(표 2) 디지털 결제 지갑의 정보저장 및 전송 방식
(Table 2) Methods of Information Storage and Transmission in Digital Payment Wallets

구분	정보저장방식	전송방식	사례
NFC	USIM	바코드 리더	앱카드, 구글 월렛 등
	마이크로 SD	NFC	애플 페이 등
	임베디드 SE		
non-NFC	서버	MST	삼성 월렛 등

디지털 결제 지갑은 일반적으로 클라이언트-서버 구조로 작동하며, 사용자 장치와 결제 서버 간에 정보를 전송하여 결제 처리를 수행한다. 이 과정에서 통신사와 금융회사가 주요 이해관계자이며, 디지털 결제 서비스는 NFC와 non-NFC 기반으로 구분된다. NFC 기반 서비스는 결제 정보를 SE(Secure Element)에 저장하고, 이를 통해 결제가 이루어지며, non-NFC 방식은 서버형 결제 방식을 사용해 일회성 결제 코드를 생성하여 거래한다. 디지털 결제 지갑은 온·오프라인 결제 인터페이스를 지원하며, NFC, MST(Magnetic Secure Transmission), QR 코드 등 다양한 전송 방식을 통해 결제를 진행한다. 특히, 모바일 결제는 스마트폰을 사용하여 오프라인 매장에서 결제를 할 수 있게 해 주며, QR 코드 및 NFC 기술을 활용하여 결제 단말기와 연결된다 [15-17].

표 2에서는 NFC 사용 여부에 따라 디지털 결제 지갑의 정보 저장 및 전송 방식이 분류되었다. 정보 저장 방식과 관계없이 전송 방식은 선택적으로 조합 가능하다. NFC 기반 서비스는 결제 정보를 저장하는 SE(보안 요소)의 구현 방식에 따라 분류된다. 이동통신사는 USIM 방식을 선호하고, 금융기관 등 서비스 제공자는 마이크로 SD 방식을 사용하며, OS 플랫폼 사업자나 휴대폰 제조사는 단말기에 SE를 내장하는 임베디드 SE 방식을 사용한다.

암호화폐 지갑은 암호화폐의 저장, 거래 기록 조회, 송금, 수신, 교환 기능을 지원하며, 개인 키와 공개 키를 사용하여 동작한다. 공개 키는 지갑 주소로 공유되어 다른 사람이 암호화폐를 보낼 수 있게 하고, 개인 키는 소유자만 알고 있어야 하며 암호화폐에 접근하고 전송하는 권한을 제공한다. 또한, 암호화폐 지갑은 거래 정보를 암호화하고 서명하는 기능을 제공한다. 2019년 기준, 약 200개의 암호화폐 지갑이 사용되며, 7,500만 명 이상의 사용자가 1,600개 이상의 암호화폐를 관리하고 있다 [18]. 비트코인 지갑은 비트코인의 잔액을 조회하고 전송하는 데 사용되지만, 실제 비트코인을 포함하지 않는다.

암호화폐 지갑은 암호화폐 거래를 위한 공개키와 개인키를 저장하는 장치, 소프트웨어 또는 온라인 서비스다. 핫 월렛은 인터넷 연결로 사용 편리하지만 보안 위험이 높고, 콜드 월렛은 보안성이 뛰어나지만 사용이 불편하다 [19-21]. 지갑은 하드웨어 지갑, 소프트웨어 지갑, 클라우드 지갑으로도 나뉜다. 하드웨어 지갑은 물리적 장치로, 소프트웨어 지갑은 앱 또는 프로그램을 통해 관리된다. 클라우드 지갑은 중요한 데이터를 클라우드에 저장하면서 사용자가 통제할 수 있게 한다. 암호화폐 거래소는 지갑 서비스를 제공하며, 수탁형 지갑(제3자가 관리)과 비수탁형 지갑(사용자가 관리)으로 구분된다. 또한, 다중 서명 방식을 통해 여러 기기에 개인 키를 분산 저장하는 방법도 있다. 대표적인 암호화폐 지갑으로는 Ledger, Trezor, MetaMask가 있다 [4, 8, 20].

암호화폐 지갑은 표 3과 같이 구현 방식에 따라 HW지갑, SW지갑 및 클라우드(서버형) 지갑으로 분류될 수 있다. 앞서 언급하였던 바와 같이 온라인, 모바일 지갑 구현은 핫월렛 범주에 속하며 종이 지갑이나 USB, 스마트 카

드와 같은 하드웨어 지갑 구현은 콜드월렛 범주에 속한다. 구현 형태 관점에서 클라우드형 전자지갑은 키와 중요 데이터를 클라우드 상에 저장하지만 사용자가 그 전자지갑의 소유권과 통제권을 갖게 된다. 많은 중앙화된 거래소에서는 사용자의 키를 직접 관리하고 사용자에게 계정을 부여한 후 계정 인증을 통해 거래를 수행할 수 있도록 한다.

(표 3) 암호 화폐 지갑의 구현 방식 분류
(Table 3) Classification of Cryptocurrency Wallet Implementation Methods

구현 방식	내용	구현 형태
SW	• 소프트웨어 지갑은 PC나 스마트폰 상에서 동작하는 프로그램 • 프로그램 설치로 쉽게 이용할 수 있으나 해킹 취약성	웹 지갑, 모바일 지갑
HW	• 별도의 물리적 장치를 사용하여 전자지갑 기능을 구현 • 암호화 키와 암호 처리를 별도의 하드웨어 내에서 수행함으로써 해킹의 취약성 경감	USB, 스마트 카드
클라우드 (서버형)	• 인터넷 상에 전자지갑 역할(주요정보 저장, SW)을 탑재하고 필요 시 활용하는 소프트웨어 서비스 • 서버 혹은 클라우드 측에서 전자지갑 주요정보 접근통제	중앙화된 거래소, 전문 지갑 서비스

4. 보안 특성 분석

전자지갑은 PC와 스마트폰 기반으로 사용되기 때문에, 이들 장치에서 발생할 수 있는 다양한 보안 위협에 노출될 수 있다. 이러한 위협은 주로 인터넷 시스템과 네트워크의 구조적 한계에서 발생하며, 대표적으로 악성코드 감염, 패스워드 탈취, 소프트웨어 취약점을 통한 공격, 피싱 등 다양한 형태의 해킹 사고가 발생할 수 있다. 이러한 위협 요소들은 대부분 1차적인 침해사고에 해당하지만, 전자지갑 해킹의 경우 더 심각한 문제를 일으킬 수 있다. 예를 들어, 사용자의 개인정보가 유출되거나 도용되는 사고가 발생하면 2차적으로 부정거래가 일어날 수 있으며, 이는 결국 금융사고로 이어질 가능성이 크다. 또한, 해커가 거래 정보를 위·변조하여 사용자에게 피해를 입히는 등의 위협도 존재한다.

전자지갑의 보안성을 높이기 위해서는 주요 위협 요소를 정확하게 식별하고, 이를 예방할 수 있는 대책을 마련하는 것이 중요하다. 전자지갑을 안전하게 사용하기 위해서는 정당한 사용자의 접근 제어가 반드시 필요하며, 사용자의 주요 정보가 안전하게 보관될 수 있는 기능이 필수적이다. 특히, 디지털 자산 시장이 급속히 확대됨에 따라 전자지갑에서 중요한 역할을 하는 개인키의 안전한 관리가 더욱 중요해졌다. 과거 인터넷 금융거래에서는 공인인증서의 개인키가 PC의 하드디스크에 저장되어 악성코드 감염 시 예금 탈취 등의 사고를 일으킨 사례가 있었다. 이처럼 개인키가 유출되면 사용자의 디지털 자산에 대한 접근이 가능해지며, 이는 금전적인 피해를 초래할 수 있다. 암호화폐 전자지갑에서도 개인키를 통해 디지털 자산에 접근할 수 있기 때문에, 개인키 관리의 중요성이 더욱 강조된다. 개인키는 사용자의 신원을 확인하고 디지털 자산의 소유권을 증명하는 중요한 요소이기 때문에, 이를 안전하게 저장하고 관리하는 것은 전자지갑 보안에서 핵심적인 역할을 한다.

디지털 ID 지갑은 사용자 인증을 강화하기 위해 멀티팩터 인증을 적용하여 ID 보호 수준을 높였으며, 모바일 결제 지갑은 결제 정보의 저장과 노출을 최소화하는 방향으로 발전했다. 또한, 암호화폐 지갑 분야에서는 최근 보안 사고를 반영하여, 사용자 개인키 남용으로 인한 부정 거래를 방지하기 위해 권한 분산형 수탁 지갑 모델의 개발이 필요하다는 요구가 커지고 있다. 기존의 전자지갑 사용 사례에서는 개인이 직접 지갑을 관리하는 방식이 기업에 비해 보안 관리가 체계적이지 못해, 공격자가 핵심 관리 정보를 탈취하고 안전하지 않은 환경에서 키를 사용해 개인 신원을 사칭하거나 부정 거래를 일으킬 위험이 있다.

전자지갑의 주요 정보 저장 방식은 각 분야별로 보안 강화를 위해 발전했다. ID 지갑은 멀티팩터 인증을 사용해 인증서와 OTP 등을 하드웨어에 구현하여 중요 정보 탈취를 방지하지만, 중간자 공격과 같은 정교한 공격에는 취약하다. 결제 지갑은 민감한 정보를 임의의 코드로 대체하여 카드 정보 노출을 최소화하고, 결제정보나 증명서를 일회용 코드로 처리하여 재사용을 방지한다. 암호화폐 지갑은 개인키를 소지 정보로 간주하고, 이를 안전하게 보호하기 위해 임베디드 SE에 저장하는 방식으로 발전했다.

정보의 가치가 증가하고 스마트폰 사용이 확산됨에 따라 전자지갑 분실 및 탈취 시 복구 및 재발급 기능의 필요성이 커졌다. 일반적으로 전자서명키가 폐기되어도 새로운 서명키로 신원을 확인할 수 있지만, 분산원장에서의

서명키는 디지털 자산에 접근하는 데 사용되므로 개인키 분실이나 도난 시 해당 자산에 접근할 수 없고 거래 취소도 불가능하다. 따라서 개인키 분실이나 탈취 시 복구 기능과 탈취된 키 폐기 후 재발급이 중요하며, 권한 분산과 같은 복구 지원 방식이 필요하다. 이는 개인키 관리의 위험을 줄이고 사기성 사용이나 남용을 방지하는 데 중요한 역할을 한다.

5. 결 론

디지털 자산의 급속한 확장에 따라, 전자지갑은 중요한 역할을 하며 다양한 분야에서 사용되고 있다. 각 전자지갑 유형은 고유한 보안 요구사항을 가지고 있으며, 이를 충족하기 위한 기술적 발전이 필요하다. 디지털 ID 지갑은 신원 정보 보호를 위해 멀티팩터 인증과 같은 고급 보안 기술을 사용하고, 디지털 결제 지갑은 결제 정보의 안전성을 강화하기 위한 다양한 방안을 채택하고 있다. 암호화폐 지갑은 개인키 관리의 중요성을 강조하며, 이를 안전하게 보호하기 위한 다양한 방식이 발전하고 있다. 특히, 개인키의 유출이나 분실 시 발생할 수 있는 보안 사고를 예방하기 위해 권한 분산형 모델이나 재발급 시스템의 필요성이 대두된다. 전자지갑의 보안을 강화하기 위한 기술적 요구사항을 식별하고, 사용자와 디지털 자산을 안전하게 보호할 수 있는 방안을 마련하는 것이 중요하다. 향후 전자지갑의 발전은 디지털 자산 관리의 중심적인 역할을 할 것으로 기대되며, 보안 기술의 발전과 함께 안전하고 효율적인 관리 시스템이 구축될 필요가 있다.

참고문헌(Reference)

[1] Deloitte, “A Market Overview of Custody for Digital Assets,” Digital Custodian Whitepaper, 2020. https://www.deloitte.com/content/dam/assets-zone2/middle-east/en/docs/services/financial-advisory/2024/me_Digital-Custodian-Whitepaper.pdf

[2] ENISA, “An Introduction to Digital Currencies and Distributed Ledger Technologies,” ENISA Report, February 2021. https://service.betterregulation.com/document/609693

[3] K.-H. Lee, “Trends in the Blockchain and Web 3.0 Technology Ecosystem,” TTA Journal vol. 200, March 2022. http://weekly.tta.or.kr/weekly/files/20223709033746_weekly.pdf

[4] S. Jokic, A. M. Cvetkovic, S. Z. Adamovic, N. Risti, “Comparative Analysis of Cryptocurrency Wallets vs Traditional Wallets.” Scientific Review Article, 2019. http://dx.doi.org/10.5937/ekonomika1903065J

[5] T.-H. Kim, “Discussion on the NFC Mobile Payment Service Ecosystem and the Role of TSM,” Press Release Korea Information Society Development Institute, October 2011. https://www.kisdi.re.kr/cmm/fileDown.do?key=147588&type=bbs

[6] J.-S. Park, “Analysis of Cybersecurity Threats and Security Requirements of Digital Wallets,” KISA Insight, December 2022. https://www.kisa.or.kr/20301?page=1

[7] IEEE Standards Association, “IEEE Standard for a Custodian Framework of Cryptocurrency,” IEEE Std 2140.5-2020, pp.1-23, July 2020. https://doi.org/10.1109/IEEESTD.2020.9144688

[8] Zakwan Jaroucheh and et.al., “Crypto Assets Custody: Taxonomy, Components, and Open Challenges,” IEEE ICBC Conference, May 2023. https://doi.org/10.1109/ICBC56567.2023.10174959

[9] Financial Security Institute, “Implementation of a Universal Secure Electronic Wallet for Digital Assets,” Research Report, November 2023. https://www.fsec.or.kr/bbs/detail?menuNo=69&bbsNo=11387

[10] Y. S. Cho, S. H. Jin, “Electronic Identity Wallet System to Provide User-Centric ID Management Facilities” ETRI Trend Report, vol. 23, no. 4, pp. 10-18, 2008. https://doi.org/10.22648/ETRI.2008.J.230402

[11] Y. S. Jung, S. H. Lim, O. Yi, J. I. Lim, S. H. Jin, “A Secure Mobile Digital ID Wallet using USIM of 3GPP,” 4th EuroFGI Workshop on Wireless and Mobility, 2007. https://recerca.ac.upc.edu/eurongi08/ext-abs/5-2.pdf

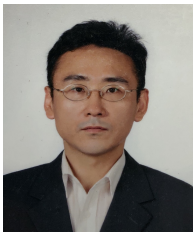
[12] S. H. Jin, “EU eIDAS 2.0 and the European Digital Identity Wallet,” TTA Journal vol. 211, pp. 90-95, January 2024. https://www.tta.or.kr/tta/preportNewsNDownload.do?sfn=20240311011443491_ZwAw.pdf

[13] S. K. Heo, “Analysis of Mobile Proximity Payment Technologies and Service Status,” Korea Financial

Telecommunications & Clearings Institute, Payment Systems and Information Technology, vol. 53, 2013.
[14] Financial Security Institute, “Research on Enhancing the Security of App Cards”, Research Report, December 2014.
[15] D. K. Lee, “Trends and Implications of Mobile Payment Innovations,” BOK Issue Note, Bank of Korea, 2013.
[16] E. -J. Steffens, A. Nennker, Zhiyun Ren, Ming Yin and L. Schneider, “The SIM-based mobile wallet”, IEEE 13th International Conference on Intelligence in Next Generation Networks, October 2009. https://doi.org/10.1109/ICIN.2009.5357095
[17] T. O. Kim, “TSM Model and Implications in Mobile Payment Services,” Korea Financial Telecommunications & Clearings Institute, Payment Systems and Information Technology, vol. 51, 2013.
[18] I. Eyal, “On Cryptocurrency Wallet Design,” Open Access Series in Informatics (OASIcs), March 2022. https://doi.org/10.4230/OASIcs.Tokenomics.2021.4
[19] KISA, “Analysis of Cybersecurity Threats and Security Requirements of Digital Wallets,” KISA Insight, 2022. https://www.kisa.or.kr/20301?page=1
[20] S. Suratkar, M. Shirole, S. Bhirud, “Crypto- currency Wallet: A Review,” IEEE 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), September 2020. https://doi.org/10.1109/ICCCSP49186.2020.9315193
[21] T. Hardjono, A. Lipton, A. Pentland, “Towards a Public Key Management Framework for Virtual Assets and Virtual Asset Service Provider,” The Journal of FinTech, vol. 01, no. 01, 2021. https://doi.org/10.1142/S2705109920500017

◐ 저 자 소 개 ◑

김 문 성(Moonseong Kim)
2002년 성균관대학교 일반대학원 수학과 (이학석사)
2023년 경상국립대학교 일반대학원 수학과 (박사수료)
2007년 성균관대학교 일반대학원 전기전자및컴퓨터공학부 (공학박사)
2007년~2009년 미국 미시간주립대학교 컴퓨터과학공학과 연구원
2009년~2018년 특허청 사무관 (서기관 대우)
2018년~현재 서울신학대학교 IT융합소프트웨어학과 교수 (행정사 / 기술거래사)
관심분야 : 모바일 센서 네트워크, 지능형 모바일 컴퓨팅, 머신러닝 및 인공지능, 정보보안, 지식재산권 등
E-mail : moonseong@stu.ac.kr



임 형 진(Hyung-Jin Lim)
2007년 성균관대학교 일반대학원 전기전자및컴퓨터공학부 (공학박사)
2007년~현재 금융보안원
관심분야 : 금융보안, 개인정보보호, 가상자산 보안 등
E-mail : hjlim@fsec.or.kr