KISA INSIGHT

DIGITAL & SECURITY POLICY

2022 **VOL. 6**

디지털 지갑의 사이버보안 위협 및 보안 요구사항 분석

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

KISA INSIGHT
DIGITAL & SECURITY POLICY
2022 VOL. 6

디지털 지갑의 사이버보안 위협 및 보안 요구사항 분석

이재성·우성도

CONTENTS

작성

한국인터넷진흥원(KISA) 보안인증단 디지털서명인증팀

이재성 팀장 02-405-5611 elemanlee@kisa.or.kr
우성도 선임연구원 02-405-4897 fresrm@kisa.or.kr

요 약

| 디지털 지갑은 기존 결제수단에서 통합 개인화 플랫폼으로 성장하고 있어, 보안 위협 증가 예상에 따른 예방책 필요

- 2011년 결제 서비스를 지원하는 수단으로 등장 후, 각종 증명서·자격증 등을 저장하는 플랫폼으로 성장 중이며, 2025년까지 다양한 산업 분야에서 글로벌 핵심 결제수단이 될 것으로 전망
- 각종 자격증명 데이터가 일원화되어 편리성과 보안성에 대한 양날의 검 이슈 존재, 보안 강화를 위한 보안 위협 분석과 그에 대한 지갑이 갖추어야 할 보안 요구사항 도출 필요

| 사용자 인증과 전자서명 서비스를 제공하는 디지털 지갑

- 디지털 지갑의 운영 형태는 다양하게 구현될 수 있으며, 현재의 디지털 지갑 운영체계를 일반화하여 ① 사용자 기기 설치형 모델, ② 제3자 위임형 모델로 분류
- 디지털 지갑은 온·오프라인 상에서 송수신 정보의 진위 확인과 검증을 위해 전자 서명키를 지갑 내에 저장하여 신원확인체계와 함께 운영

| 참여주체 별, 데이터 송수신 과정에서 다양한 보안 위협 발생 예상

- 디지털 지갑에 저장된 개인정보와 전자서명키 탈취 시, 사용자의 신원도용, 금전적 손해, 각종 범죄 노출 등 광범위한 2차 피해 발생 가능성 존재
- 보안 위협은 사회공학, 취약점 공격 등으로 사용자, 지갑 서비스 제공자, 발급자, 기기 및 시스템, 서비스 제공자 기기 등에서 다양하게 발생할 것으로 예상

| 다양하게 발생하는 보안 위협에 대응하기 위한 보안 요구사항 도출

- 기존 평가기준으로부터 ① 공통 보안, ② 서비스 보안, ③ 개인정보보호 측면에서 보안원칙과 관련 법을 준수할 수 있는 보안 항목 도출
- 향후 디지털 지갑에 저장·전송되는 데이터 형식, 신원확인체계, 신원확인의 신뢰성 수준, 인증 수단 등, 다양한 관점이 고려된 지속적인 현황 조사 및 연구 필요

Ⅰ 디지털 지갑 개요

■ 디지털 지갑, 글로벌 핵심 결제수단으로 성장 중

| 디지털 지갑 서비스의 등장과 성장

- 2011년 구글이 처음 마스터카드를 모바일 기기에 저장하여 전자상거래에 이용하는 '구글 월렛' 서비스를 발표한 이후 애플, 아마존, 삼성 등 글로벌 기업을 주축으로 간편결제 서비스가 활성화
- 현재 국내에는 금융, 유통, 제조 분야 등에서 핀테크 기업과 빅테크 기업 주도로 간편 결제 서비스 뿐 아니라 각종 행정 증명서나 자격증, 전자서명 인증서를 지갑 앱에 등록해서 사용자가 이용하고자 하는 서비스에 활용하는 형태로 디지털 지갑의 기능이 확장됨
- 최근 글로벌 리서치 기관의 조사 결과[1], 2025년까지 전 세계적으로 디지털 지갑이 전자상거래 부문에서 핵심 결제 수단으로 성장할 것으로 전망하고 있어, 향후 국내에서도 다양한 산업 분야 및 서비스에서 디지털 지갑이 활용될 것으로 기대

| Trade-off 위협, 편리성 vs 보안성

- 디지털 지갑은 사용자의 금융·개인정보 등이 일원화되는 특징으로 인해 사용자 입장에서는 편의성이 높아지나, 해킹사고 발생 시 개인정보 유출로 인한 광범위한 대국민 피해로 이어져 국가적 혼란이 발생할 가능성이 높으므로 사고 예방을 위한 보안 위협 식별과 사전 대응 필요
- 디지털 지갑 보안 강화를 위해 제Ⅱ장에서 디지털 지갑 정의와 운영체계를 논의하고, 제Ⅲ장에서는 디지털 지갑의 운영체계에서 발생할 수 있는 잠재적인 보안 위협과 참여 주체별 대응방안을 논의
- 제Ⅳ장에서는 제Ⅲ장에서 식별된 보안 위협을 예방하기 위해 기존 평가기준으로부터 디지털 지갑이 갖추어야 할 보안 요구사항을 도출

1. FIS, "The global payments report", 2022, pp. 6-11.

Ⅱ 디지털 지갑 정의 및 운영체계

■ 디지털 지갑 현주소, 기술 개방성 및 다양성

| 온·오프라인 인증 & 전자서명 생성 서비스, 디지털 지갑 정의

• 전자지갑(Electronic wallet), 디지털 지갑(Digital wallet), 디지털 화폐 지갑 (Digital currency wallet) 등 다양한 용어로 사용되고 있는 지갑의 정의를 선진적인 전자신원관리 법체계로 인정받고 있는 유럽연합(EU)의 최신 eIDAS 개정안을 통해 확인

[표 1] EU 디지털 신분증 지갑(Digital Identity Wallet)

구분	내용
정의	개인의 신원 관련 정보를 저장하고 온·오프라인 인증을 위해 사용하고 신뢰된 제 3자를 통한 전자서명과 인장을 생성하는데 활용할 수 있는 제품이나 서비스(제3조 제42호)
발급 대상	EU 내 모든 자연인 및 법인(제6a조 제1항)
발급 비용	자연인은 무료(제6a조 제6항), 법인은 미정
발급자	① 정부가 직접 발급 ② 정부로부터 위임받은 기관 ③ 정부의 인정을 받은 (민간)독립기관(제6a조 제2항) * 발급자가 ②, ③에 해당하는 민간기관인 경우, 별도 법인이어야 함(제6a조 제7항, 제45f조 제4항)
지갑 기능	① 사용자에게 투명하고 추적 가능한 방식으로 인증에 필요한 식별정보와 속성증명서를 안전하게 요청, 획득, 저장, 선택, 결합, 공유할 수 있는 기능 ② 신뢰된 전자서명수단에 의한 서명 기능(제6a조 제3항)
사용자 보호 기능	사용자는 디지털신원 지갑을 완전 통제할 수 있어야 함(제6a조 제7항) * 지갑발행자는 사용자의 명시적 요청 없이 지갑 서비스 제공에 필요하지 않은 지갑 사용에 관한 정보 수집 금지, 개인식별정보를 개인데이터와 결합 금지, 디지털신원지갑 제공과 관련된 개인 데이터는 보유 중인 다른 데이터와 물리적·논리적 분리 보관 등

(출처) 필자 작성

- 디지털 지갑은 특정 기술이 적용된 서비스를 지칭하는 것이 아니며, 지갑 서비스 제공자가 구현하고자 하는 방식에 따라 사용자의 모바일 기기에 지갑 앱을 설치하는 어플리케이션 유형이나 데스크톱 또는 모바일 기기 등을 통해 원격으로 온라인 지갑 서비스에 접속하는 유형, 물리적 카드에 정보를 저장하는 스마트카드처럼 다양한 방식으로 구현
- 본 보고서에서는 현재 가장 많이 사용되고 있는 유형인 삼성페이, 애플페이 등의 간편 결제 서비스와 W3의 DID 기반의 모바일 신분증을 포함하여 네이버NA, 카카오톡 지갑 등의 전자문서 지갑을 구현하는 소프트웨어 기반의 디지털 지갑을 설명

[표 2] 국내 디지털 지갑 현황

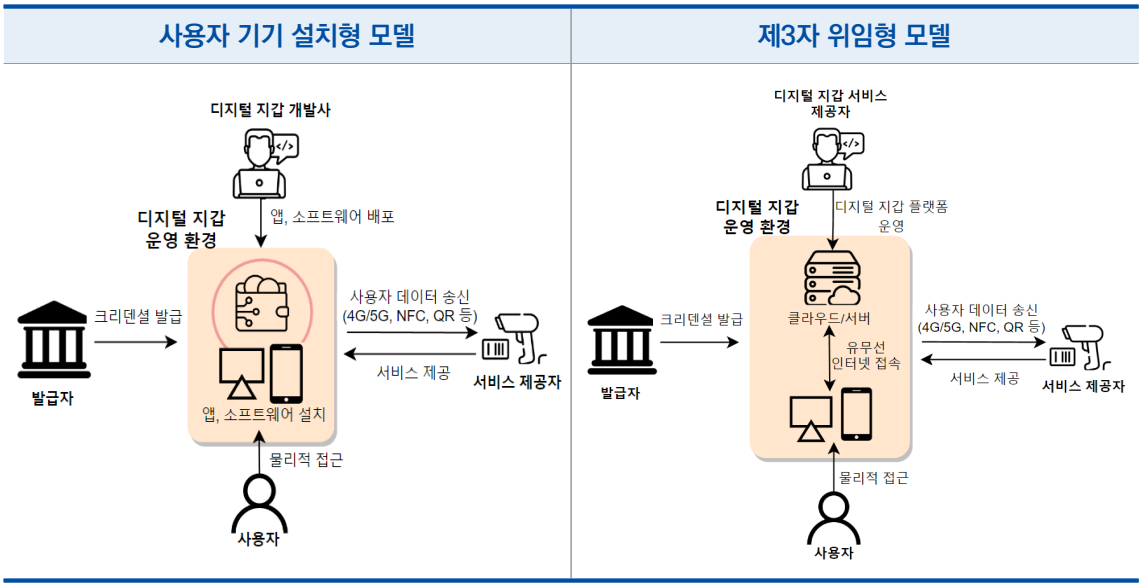
디지털 지갑 사업자	인증서	공공 연계서비스	자체 서비스
카카오톡 지갑	카카오 인증서	① 신분증/자격증 ② 전자증명서 7종	① 출입증/보증서 ② 디지털 명함 ③ 개인 데이터 보관 (톡 데이터)
네이버NA	네이버 인증서	① 전자증명서 16종 ② 전자고지서 8개	① 출입증 ② 간편 결제 수단 ③ 쇼핑, 예약, 쿠폰, 멤버십 제휴 포인트
비바리퍼블리카 TOSS 지갑	TOSS 인증서	① 자격증 ② 고지서 ③ 전자증명서 30종	① 신용점수관리 ② 보험 조회, 병원비 돌려받기 ③ 부동산, 자동차 등 자산관리

(출처) 필자 작성

| 어플리케이션 vs 원격접속, 디지털 지갑의 운영체계

- 디지털 지갑에서 발생할 수 있는 보안 위협을 식별하기 위해 우선적으로 지갑의 운영체계 파악 필요
- 운영체계는 지갑의 운영 환경에 따라 2가지 유형으로 일반화하여, 사용자 기기 설치형 모델과 제3자 위임형 모델로 구분
- 디지털 지갑은 사용자, 자격증명 발급자, 제3의 서비스 제공자 등 참여자들로부터 송·수신되는 정보의 진위 확인과 검증을 위해 전자서명키를 지갑 내에 저장하여 신원확인체계와 함께 운영됨
- 디지털 지갑의 참여 주체들은 PKI와 최근 블록체인 기반의 DID 등의 신원확인체계를 통해 크리덴셜이 정당하게 발급된 사실과 다른 참여 주체들을 검증

[그림 1] 디지털 지갑 운영체계



(출처) ENISA, “Security of Mobile Payments and Digital Wallets”, 2016. 12.
TTAK.KO-12.0359-Part1, “분산ID를 활용한 신원관리 프레임워크 제1부”, 2020. 12. 10.
ISO/IEC, “18013-5 Part 5: Mobile Drive License, mDL”, 2021. 9.
윤대근, “자기주권 신원증명 구조 분석서”, 제이펍, 2020.
TTA저널 199호, “탈중앙화 신원관리 서비스 모델”, 2022. 1.
W3C, https://www.w3.org/TR/vc-data-model, 참고 재구성

- 사용자 기기 설치형 모델은 사용자가 자신이 소유한 기기에 디지털 지갑 개발사가 개발·배포한 어플리케이션을 설치한 후, 발급자로부터 크리덴셜을 발급받아 기기에 저장
- 이후 사용자는 이용하고자 하는 서비스에 신원검증 등이 필요할 때 해당 서비스 제공자에게 크리덴셜을 제출
- 제3자 위임형 모델은 디지털 지갑 서비스를 사용자의 기기가 아닌 지갑 서비스 제공자가 자체 운영하는 정보시스템 또는 클라우드 사업자가 운영하는 환경에서 지갑 서비스가 운영되는 형태로, 사용자는 인터넷을 통해 자신의 기기를 사용하여 원격으로 지갑 서비스를 접속 및 이용
- 크리덴셜 데이터가 저장되는 위치는 사용자의 개인정보 데이터와 전자서명키를 모두 제3자의 디지털 지갑 운영 환경에 저장하거나, 전자서명키만 사용자 기기에 저장하는 방식 또는 개인정보 데이터와 전자서명키를 상호간에 저장하는 백업 형태로 운영

[표 3] 사용자 기기 설치형 모델 VS 제3자 위임형 모델

구분		사용자 기기 설치형 모델	제3자 위임형 모델
참여 주체	사용자	- 본인이 소유한 기기에 디지털 지갑 앱 설치 - 발급자로부터 발급받은 크리덴셜 데이터를 디지털지갑 앱에 저장	- 필요 시 사용기기에 디지털 지갑 앱 설치 - 발급자로부터 발급받은 크리덴셜 데이터를 기기에 저장 or 원격 디지털지갑 환경에 저장
	디지털 지갑 사업자	(디지털 지갑 개발사) - 디지털 지갑 어플리케이션 개발·배포 - 크리덴셜 데이터를 저장·운용할 수 있는 어플리케이션 환경 개발	(디지털 지갑 서비스 제공자) - 사용자가 원격에서 접속 가능한 디지털 지갑 환경(서버/클라우드 등) 구성 - 크리덴셜 데이터를 저장·운용할 수 있는 시스템 환경 구성 - 사용자 요청 시 크리덴셜 데이터를 서비스 제공자에게 전송
	발급자	- 사용자가 크리덴셜 데이터 요청 시, 사용자 기기로 크리덴셜 데이터 전송	- 사용자가 크리덴셜 데이터 요청 시, 사용자 기기 or 지갑 서비스 제공자가 운영 중인 디지털 지갑 환경(서버/클라우드 등)으로 전송
	서비스 제공자	- 근거리 통신 프로토콜(NFC, MST, 블루투스 등) or 유무선 네트워크(4G/5G, WiFi 등)를 통해 QR 코드 등을 사용하여 사용자의 크리덴셜 정보 송수신 - 사용자가 제출한 크리덴셜 정보를 신원확인체계를 통해 검증 후 사용자에게 전자상거래 등 서비스 제공	
특징		- 사용자의 크리덴셜 데이터를 사용자가 소유한 기기에 저장	- 사용자의 크리덴셜 데이터를 원격 디지털 지갑 환경(서버/클라우드 등)에 저장
장점		- 크리덴셜 데이터의 저장 위치가 비교적 투명함	- 디지털 지갑 사업자에 의해 일정 수준의 보안성 제공 - 백업, 복구 등 관리 용이
단점		- 사용자 부주의로 인한 피싱, 멀웨어 감염 등에 노출 가능성 존재 - 도난, 분실 가능성 존재	- 크리덴셜 데이터의 저장 위치가 비교적 불투명함 - 서버 탈취 시 다수의 사용자 크리덴셜 정보 유출 가능성 존재

(출처) 필자 작성

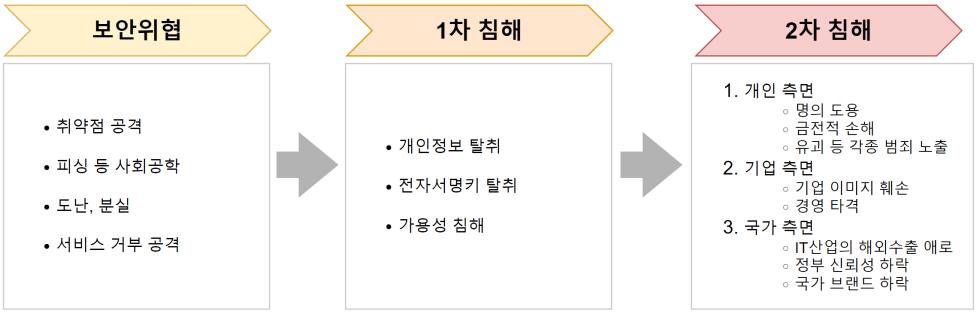
Ⅲ 디지털 지갑 보안위협 분석

■ 디지털 지갑에 저장된 개인정보 탈취로 인한 사용자의 생명과 재산을 위협하는 2차 피해 양산 우려

| 개인정보가 흐르는 블루오션, 디지털 지갑

- 디지털 지갑의 보안위협을 살펴보기에 앞서 디지털 지갑이 공격 목표가 되는 이유를 살펴보면 개인정보 탈취, 전자서명키 탈취, 서비스의 가용성 침해 3가지로 나누어 짐
  - **(개인정보 탈취)** 복수의 발급자로부터 발급받은 사용자의 다양한 개인정보가 지갑에 일원화되어, 단 한번이라도 공격에 성공하면 사용자의 다양한 정보가 탈취되어 2차 피해로 이어짐
  - **(전자서명키 탈취)** 전자서명키는 사용자가 제출하는 정보에 대해 부인방지와 서명자 확인 기능을 제공하여 온라인 환경에서 사용자의 신원과 특정 행위를 증명하는 용도로 사용되는 중. 전자서명키가 탈취되는 경우 공격자가 사용자의 신원을 도용하여 전자상거래, 의료, 정부 민원정보 등을 악용한 광범위한 피해로 이어짐
  - **(가용성 침해)** 사용자가 특정 서비스를 이용하기 위해 디지털 지갑에 저장된 자신의 정보를 제공하는 시점에 자격증명을 불가능하게 만들어 사용자의 지갑 서비스 이용이 불가능한 피해 유발 가능

[그림 2] 개인정보 침해 경과

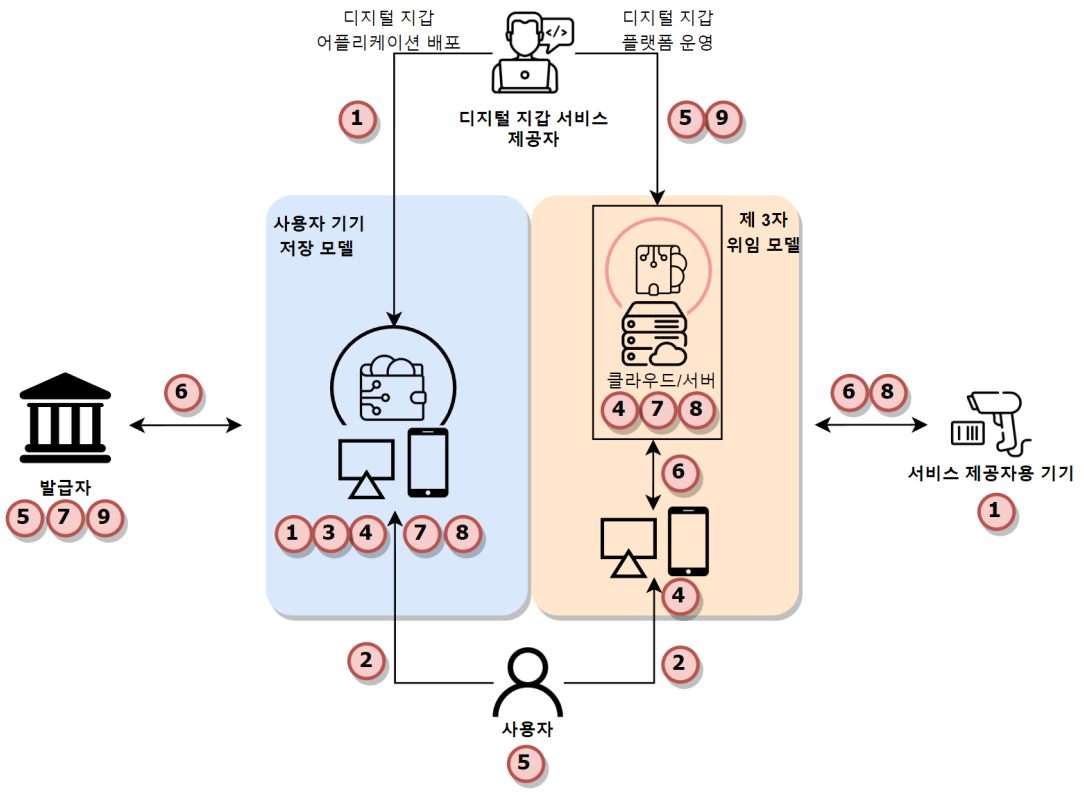


(출처) 개인정보보호 포털 “개인정보 침해에 따른 피해”, 참고 재구성

| 디지털 지갑의 공격 벡터

• 디지털 지갑에서의 보안위협이 발생 지점을 살펴보기 위해 앞서 설명한 운영체계상에 보안위협의 발생 위치(그림 3)를 표시하고, 각 보안위협에 대한 예시(표4)를 참고

[그림 3] 디지털 지갑 보안위협 발생 예상 지점



(출처) ENISA, “Security of Mobile Payments and Digital Wallets”, 2016. 12.
한국인터넷진흥원, “사이버 위협 동향보고서(2021년 상반기)”, 2021.
OWASP, “OWASP Mobile Top 10”, 2022.
IC3, “Multiple Vulnerabilities in BLE Devices”, 2022. 11.
MITRE, “CWE Top 25 Most Dangerous Software Weaknesses”, 2022. 참고 재구성

[표 4] 보안위협 예시

보안위협	예시
① 위조 어플리케이션 & 멀웨어	- 사용자가 피싱 이메일에 첨부된 악성 첨부파일을 열거나 악성 URL 클릭 시 악성코드 다운로드 및 감염(드라이브 바이 다운로드) - POS기의 취약점을 악용한 멀웨어 설치 - 스토어로부터 다운로드 받은 어플리케이션을 언패킹 후 루틴을 변조·패킹하여 스토어에 업로드 - 공급망 공격을 통해 악성코드에 감염되어 배포된 어플리케이션, 패치 파일 설치
② 도난, 분실	- 공격자가 습득한 기기에 포렌식 툴을 이용하여 관리자 권한 및 저장 정보 탈취 - 공격자가 취약한 인증이 적용된 기기를 습득한 경우 관리자로 로그인 후 저장된 정보 탈취
③ 역공학	- 소스코드 분석을 통한 취약점(하드코딩 PW, 암호화 키 등) 스캐닝
④ 취약점 공격	- 취약한 API 사용으로 인해 발생하는 허가되지 않은 접근 - 취약한 암호 알고리즘 사용으로 인한 저장·전송 정보 노출 - 해시 충돌로 인한 PW 노출 - 하드코딩된 PW, 암호화 키 유출 - 딥링크 검증 미흡으로 공격자의 임의 명령어(로그인 정보 캡처) 실행, 공격자 서버 전송 - SQL 인젝션, 버퍼오버플로우로 인한 메모리에 저장된 개인정보 유출, 임의 명령 실행 - 근거리 통신 프로토콜의 취약점을 악용한 보안 검증 우회 - 자원에 대한 접근 권한 검증이 미흡하여 카메라, 스피커 등 기기의 자원에 접근하여 사진, 녹음 데이터를 공격자 서버로 전송
⑤ 피싱/사회공학	- 피싱 이메일, SMS, 이메일, SNS, 검색엔진 등을 통한 카드정보, 이름, 생년, 연락처, 배송지, 주소, 이메일, 핸드폰 번호 노출 - 신원을 도용한 악의적 사용자에게 1:1 자산 송금 - 서버에 접근 권한을 가진 내부자의 결탁·부주의로 인한 사용자의 크리덴셜 정보 유출
⑥ 중간자 공격	- SSL/TLS, VPN, 종단간 암호화가 되지 않은 데이터 탈취 - 변조된 악성 QR 코드를 사용자에게 전송하여 스캔 시 공격자의 임의 명령어 실행 - NFC, MST, BLE 등 근거리 통신 프로토콜 취약점을 악용한 메시지 무결성 훼손 - 기기·서버 및 수신기(POS 등) 간 트래픽 분석, 스니핑 등으로 인해 발생하는 정보 노출 - 스푸핑을 통한 세션키 탈취 등 정보 유출 - 스니핑을 통해 탈취한 인증정보 또는 미흡하게 처리된 토큰을 재전송하여 사용자 신원 도용 및 서비스 무단 이용
⑦ 사용자 크리덴셜 이슈	- APT 공격을 통해 멀웨어 설치 후 사용자의 기밀정보를 C&C 서버로 전송 - DB에 접근권한을 가진 내부 직원에 의한 사용자의 크리덴셜 정보 탈취 - 도난된 카드 등 결제 정보 등록, 계정 프로파일 변경(연락처, 이메일, 핸드폰 번호 등) - 도난/분실 기기 or 온라인 접근을 통해 사용자 프로파일에 허가되지 않은 접근

(출처) ENISA, “Security of Mobile Payments and Digital Wallets”, 2016. 12.
한국인터넷진흥원, “사이버 위협 동향보고서(2021년 상반기)”, 2021.
OWASP, “OWASP Mobile Top 10”, 2022.
IC3, “Multiple Vulnerabilities in BLE Devices”, 2022. 11.
MITRE, “CWE Top 25 Most Dangerous Software Weaknesses”, 2022. 참고 재구성

| 구성 객체 별 대응 방안

- 디지털 지갑의 운영체계에서 주요 구성 객체 별 보안 위협의 대응방안은 아래와 같이 구분 가능
- 주요 구성 객체는 앞서 2장에서 설명한 지갑 운영체계로부터 사용자, 사용자 기기, 디지털 지갑 어플리케이션, 서비스 제공자 기기, 발급자, 디지털 지갑 서비스 제공자로 구분

[표 4] 구성 객체 별 보안위협 대응 방안

구성 객체	보안 위협	대응 방안
사용자	사회공학	- 사용자 보안 교육 - 최신 보안 업데이트 - 탈옥, 루팅 등 금지
	위조 어플리케이션 & 멀웨어 설치	
기기	도난, 분실	- 원격 기기 잠금 및 데이터 삭제 - 인증 강화(생체 인증 등) - 최신 OS·백신 프로그램 등 보안 업데이트 - 기본 보안 기능·설정 적용
	참조 모니터 매커니즘 우회	
지갑 앱·소프트웨어	보안 기능 우회	- 시큐어 코딩 적용 - 난독화 - 안티 역공학 기능 적용 - 탈옥 탐지 기능 적용 - 화이트박스 암호화 - 실시간 감시 기능 상시 활성화 - 허가되지 않은 앱 설치 금지
	크리덴셜 유출	
서비스 제공자 기기	멀웨어 감염	- 기본 보안 설정 변경(PW 등) - 최신 POS 소프트웨어 설치 - 최신 버전 프로토콜 적용 - IPS, 방화벽, 안티 DoS 등 보안 솔루션 적용 - 전송 정보 암호화(SSL 등 보안 프로토콜 적용) - QR 코드 등 무결성 검증 및 상호 인증 기능 적용
	중간자 공격	
	서비스 거부	
발급자	부정발급	- 인증 강화(추가 인증, 다중 인증 수단 적용 등) - 발급 시스템에 대한 최소 접근 권한 적용 - HSM(하드웨어 보안 모듈에 키 암호화 저장) - 멀웨어 탐지 및 방지 기능 적용 - FDS 적용 - 관리자 권한 관리(최소 권한 등)
	내부자 보안	
지갑 서비스 제공자 (서버, 클라우드, 어플리케이션, 소프트웨어)	크리덴셜 유출	- 인증 강화(다중 요소 인증 등) - 멀웨어 탐지 및 차단 시스템 배치 - 관리자 권한 관리(최소 권한 등) - 운영 웹페이지에 대한 시큐어 코딩 적용 - 최신 보안 업데이트 적용(가상화 환경, OS, 보안솔루션 등) - IPS, 방화벽, FDS, 안티 DoS 등 보안 솔루션 적용
	서비스 거부(DDoS)	
	크리덴셜 임의 정보 변경	
	공급망 공격	

(출처) ENISA, “Security of Mobile Payments and Digital Wallets”, 2016. 12.
MITRE, “D3FEND”, 2022. 참고 재작성

Ⅳ 디지털 지갑 보안 요구사항 분석

■ 운용 기기·시스템, 서비스, 개인정보보호 측면으로 분류

| 침해사고 예방을 위해 보안기술·기능 측면, 관리·이용 측면, 컴플라이언스 측면 고려

- (공통 보안) 사용자 기기와 디지털 지갑 어플리케이션, 관련 정보시스템이 지갑 서비스 이전에 고려되어야 하는 사항을 공통평가기준 등으로부터 도출한 보안 요구사항 항목
- (서비스 보안) 디지털 지갑 어플리케이션 배포 또는 사업자에 의해 지갑 서비스가 제공되는 시점에서 고려되어야 하는 보안 요구사항 항목
- (개인정보보호) OECD 프라이버시 8원칙과 Privacy by Design 7원칙을 고려하여 지갑 서비스 가입부터 이용, 제공, 폐기 과정의 개인정보 처리 단계에서 필요한 보안 요구사항 항목

[표 5] 디지털 지갑 보안 요구사항

구분		보안 요구사항
공통보안	접근통제 (식별 및 인증)	- 정당한 사용자임을 확인할 수 있는 고유 ID 식별 및 인증 기능 - 사용자 인증 실패 횟수가 임계값 초과 시, 식별 및 인증 기능 비활성화 - 관리자 인증 실패 시 관리자가 즉시 확인할 수 있는 수단을 통한 통보 기능 - 사용자 인증 정보 재사용 방지 기능(타임 스탬프, 세션 ID 암호화 등) - 인증 실패 시, 실패 사유를 추측할 수 있는 정보 제공 금지 - 인증 정보 표시 금지 기능(“*”로 대체 표시, 메모리에 평문 노출 금지 등) - 관련 서버와 통신 시, 해당 서버에 대한 식별 및 인증 - 마이크, GPS, 카메라 등 자원 접근에 대한 권한 검증

구분		보안 요구사항
	보안 관리	- (서버) 인가된 관리자에게 보안 기능(사용자 관리, 패스워드, 업데이트, 세션 관리 등)을 관리할 수 있는 보안 규칙 추가·삭제 ·변경 기능 - (서버) 관리접속에 대한 활성화·비활성화 기능 - (서버) 보안 관리를 위한 접속 호스트 제한 - (서버) 사용자 최초 접속 시 기본 패스워드 강제 변경·생성 - (기기) 사용자가 보안 기능·정책 및 중요 데이터 등 설정·관리 기능
	데이터 보호	- 데이터 전송 및 관리접속 시 암호통신 채널 사용 - 중요정보를 암호화, 접근통제 등의 방식을 적용하여 안전하게 저장 - 보안 설정값(보안 정책, 환경설정 파라미터 등)을 비인가 접근으로부터 보호 기능
	자체 보호	- (서버) 주요 프로세스에 대한 정상 실행 확인 등 자체 보호 기능 - (기기) 동작 초기화 단계에서 지갑 어플리케이션의 설정값 및 무결성 검증 - (기기) 지갑 프로세스의 임의 종료 방지 기능 - (기기) 역공학 프로그램 실행 시 자동 종료 등 안티 역공학 기능 - (기기) 예외상황(통신 차단, 비행 모드)에서도 정상적인 기기 보호 기능 - (기기) 비인가 어플리케이션 설치·삭제·변경 방지 기능 - (기기) 실시간 루팅·탈옥 탐지 및 멀웨어 감염 탐지 기능 - 설정값 및 라이브러리, 프로세스, 실행파일 등의 무결성 검증 기능 - 운영체제 변조 탐지 및 대응 기능 - 보안 프로그램 상시 실행
	업데이트 보호	- 업데이트 설치·적용 전 업데이트 파일의 유효성 검증 - 명칭, 버전, 릴리즈 등의 식별 정보를 사용자가 확인할 수 있는 기능 - 업데이트 실패 시 기존 버전 유지 기능 - 업데이트 서버 주소에 대한 무결성 확인
	세션 관리	- 사용자 세션 연결 후, 일정 시간 경과 시 세션 잠금 또는 종료 기능 - 사용자 계정 또는 동일 권한으로 중복 접속 제한
	감사 기록	- (서버) 감사기록에 불필요 정보 포함 금지 - (서버) 신뢰된 시간 정보를 이용하여 감사기록 생성 - (서버) 인가된 관리자만이 감사기록 조회, 다양한 조건 및 검색·정렬 기능 - (서버) 감사기록 무결성 보호(임의 삭제·변경 금지, 손실 방지 기능) - 보안관리, 업데이트 보호 등 주요 감사사건에 대한 기록 생성
	암호화	- 크리덴셜 데이터 전송 및 저장 시, 국내외 표준기관에서 권고하는 보안 강도가 높은 안전한 알고리즘 적용 - 대칭키·공개키 알고리즘, 해시함수 별 보안강도가 입증된 안전한 키 길이 적용 - 암호키 생명주기(생성, 분배, 저장, 정지, 폐기) 단계 별 무결성 및 기밀성 확보 - 암호키 유형(대칭키, 서명키 등) 별 권장 유효기간 설정

구분			보안 요구사항
	취약성 대응		- 시큐어 코딩 적용 - 알려진 보안 취약점(CVE, NVD 등) 제거 - 불필요 서비스 제거 또는 중지
	위험 관리		- 기기·계정 도난/분실 시 원격 잠금·해제·삭제·초기화 기능 - 분실 시 네트워크 접근 차단 및 지갑 어플리케이션 불능화 기능 - 소유자 외 사용자의 디지털지갑 재활성화 방지 기능
서비스 보안	관리적 보호조치	설치 시	- 지갑 어플리케이션은 지정된 위치에만 설치 - 기 설치된 지갑 어플리케이션 존재 시 사용자의 동의에 의해 재설치 또는 중지 - 설치 파일에 대한 무결성 검증 기능
		실행 시	- 저장된 크리덴셜은 사용자 요청 시, 안전한 방법으로 조회, 변경, 삭제 - 크리덴셜 정보 조회 시, 사용자가 선택한 정보만 출력 - 인증정보는 분리·보호된 공간(SE, TEE 등)에서 실행 - 사용자 인증 수단 생성 규칙, 변경 주기, 인증 실패 허용 횟수 설정 기능 제공
		종료 시	- 사용자가 종료 요구 시, 즉시 종료가 보장되어야 함 - 지갑 어플리케이션 종료 시, 지갑 서비스에서 사용된 데이터는 즉시 삭제되어야 함 - 데이터 접근 권한 불필요 시 즉시 권한이 제거되어야 함 - 불필요 크리덴셜 정보는 즉시 삭제되어야 함
		삭제 시	- 지갑 어플리케이션 삭제 시 안전한 방법(복구 불가능)으로 크리덴셜 데이터 삭제
	이용 시 보호조치	로그인/로그아웃 시	- 중복 로그인 시, 기존 로그인 세션에 대한 로그아웃 고지 및 새로운 로그인 세션에 대한 중복 로그인 고지 - 사용자 로그인 시 인증(PW, PIN, OTP, 생체인증 등) 기능
		가입/탈퇴 시	- 지갑 서비스 가입 시 개인정보 수집 시 보호조치 적용 - 지갑 서비스 탈퇴 시 안전한 방법으로 크리덴셜 데이터 삭제
		실행 시	- 지갑 어플리케이션 임의 호출 금지(허가된 사용자에 의해서만 호출) - 지갑 어플리케이션 실행 시 안전한 사용자 인증 기능 제공(PW, PIN, OTP, 생체인증 등) - 등록 및 인가된 저장매체만 사용
		종료 시	- 사용자의 요청에 의해서만 지갑 어플리케이션 종료 - 지갑 어플리케이션 종료 시, 지갑 서비스에서 생성된 정보 삭제

구분			보안 요구사항
개인정보 보호	수집 시 보호조치	이용 및 수집 제한	- 발급하는 크리덴셜 데이터의 소유자와 지갑 사용자의 신원 일치 여부 검증 - 안전한 인증 수단 및 절차 적용 - 지갑 서비스 가입 시 실명 인증 후 인증정보 즉시 삭제 - 지갑 서비스 가입 시 주민등록번호 대체 인증 수단 적용
	보유·이용 시 보호조치	표시 제한 및 보호 기능	- 개인정보 마스킹 - 화면 캡쳐 방지 - 푸시 알림 시 개인정보 표시 방지 - 일정 시간 후 자동 로그아웃, 화면 잠금 - 개인정보 접근 시 사용자 인증(PW, PIN, OTP, 생체인증 등) - 지갑 어플리케이션이 저장 정보·기능 접근 시 접근 권한 동의 기능 - 지갑 어플리케이션 종료 시, 버퍼 초기화
		최신성·정확성·완전성 보장	- 개인정보 변경 시 본인확인 기능 적용 - 휴면 해제 시 회원정보 업데이트 기능 구현
		안전한 보관	- 크리덴셜 정보를 일정 기간 이용 중지 시, 논리·물리적 분리 보관
	제공 시 보호조치	이용 제한 및 목적 명확화	- 제 3자에게 개인정보 제공 시 최소한의 정보 제공 - 개인정보 전송 시 사용자의 동의하에서만 전송 - 전송하는 개인정보 항목에 대해 사용자가 인지할 수 있는 표시 기능
		안전성 확보 조치	- 제공을 요청한 자의 권한 검증, 상호 인증, 접근 통제 - 접속 기록 보존
	파기 시 보호조치	안전한 삭제	- 회원 탈퇴, 사용자 요청 등으로 개인정보 삭제 시, 데이터 복원이 불가능한 초기화 또는 덮어쓰기 방식으로 즉시 삭제 - 개인정보 파기 기록 보존

(출처) 국가정보원, “(1, 2편) 국가용 보안요구사항 V3.0 – 해설 및 공통 보안 요구사항”, 2021.
한국인터넷진흥원, “암호 알고리즘 및 키 길이 이용 안내서”, 2018.
한국인터넷진흥원, “암호 키 관리 안내서”, 2016.
행정안전부, “모바일 대민서비스 보안취약점 점검 가이드”, 2021.
한국인터넷진흥원, “ID관리 서비스에서의 안전성 및 호환성 검증 방안 연구”, 2008.
행정안전부, “개인정보 처리단계별 기술적 보호조치 가이드라인”,
한국인터넷진흥원, “정보보호 및 개인정보보호 관리체계(ISMS-P) 인증기준 안내서”, 2022. 참고 재구성

V 결론

■ 온·오프라인의 개인화 플랫폼으로 성장 기대

| 메타버스의 핵심기술이 될 디지털 지갑

- 디지털 지갑에 기존 플라스틱 결제카드와 신분증, 각종 증명서 등을 일원화하여 사용하게 되면서 교통, 행정, 복지, 의료 등 다양한 온·오프라인과 메타버스 환경에서도 지갑이 활용될 것으로 기대
- 이에 따라 다양한 사용자 개인정보를 담는 플랫폼으로서, 장기적으로 디지털 지갑 간의 상호연계나 정보 공유 등의 증가로 디지털 지갑에 대한 보안의 중요성은 더욱 커질 것으로 전망

■ 지속적인 기술 연구 & 보안 이슈 예방책 마련 필요

| 민·관 협력체계 구축

- 국내 디지털 지갑 관련 민·관 협력체계를 통해 상호연계와 데이터 공유를 위한 운영체계, 기술 규격 조사 분석 연구가 지속적으로 진행되어야 함
- EU의 eIDAS, EBSI의 디지털 지갑 기능 요구사항 마련에 따른 국제적 흐름을 반영하여 디지털 지갑에 저장·전송되는 데이터 형식, 신원확인체계, 신원확인의 신뢰성 수준, 인증 수단, 송·수신 프로토콜, 통신 인터페이스에 대한 규격과 관련 정보시스템의 유형 등에 대한 현황 조사 필요

| 보안 이슈 연구 및 보안 가이드 마련

- 안전한 디지털 지갑 생태계 조성을 위해 보안 사고를 사전 예방하는 보안 요건의 기준 마련 필요
- 민·관 협력체계를 통한 위협사례 공유와 대응방안 연구가 필요하며, 이를 통해 도출된 보안 요구사항을 준수하는 세부 가이드가 개발된다면 안전한 디지털 지갑 서비스 환경을 구현할 수 있는 기반이 마련될 것으로 전망

KISA INSIGHT

DIGITAL & SECURITY POLICY

2022 **VOL. 6**

디지털 지갑의 사이버보안 위협 및 보안 요구사항 분석

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY