TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx/R1

제정일: 20xx년 xx월 xx일

분산원장기술 전자지불시스템 보안위협 및 요구사항

Security threats and requirements for digital payment systems based on distributed ledger technologies

한국정보통신기술협회
Telecommunications Technology Association

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

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	오경희	TCA서비스	대표/분산원장 기술표준포럼 연구책임자	PG 502 위원	
표준 초안 작성자	김동진	금융보안원		-	
	류재철	충남대학교	교수	-	
사무국 담당		TTA		-	

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 : 20xx.xx

서 문

1 표준의 목적

이 표준의 목적은 분산원장기술에 기초한 전자 지불 시스템의 보안 위협을 분석하고 이에 대응하기 위한 보안 요구사항을 제시하는 것이다.

이 표준은 분산원장기술에 기초한 전자 지불 시스템을 운영하는 기관이 안전한 서비스 제공에 대한 보안 위협 및 보안 요구사항을 확인하고 해당 요구사항을 만족하는 해결책을 개발하는데 활용할 수 있다.

2 주요 내용 요약

이 표준은 분산원장기술에 기초한 전자 지불 시스템을 무허가형(permissionless) 및 허가형(permissioned) 분산원장 시스템 모델로 나누어 개관한다. 또한 분산원장 기반 전자지불시스템에 대한 보안 위협을 전자지불 시스템에 대한 보안 위협 및 분산원장에 대한 보안 위협으로 나누어 분석한다. 이러한 위협에 대한 보안 요구사항을 식별하고 분산원장 기반 전자지불시스템의 구성요소 별로 보안 요구사항을 상세화한다. 마지막으로 이러한 요구사항이 무허가형 및 허가형 분산원장 시스템 모델에서 달성될 수 있는 방안을 검토한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

해당사항 없음

3.2 인용 표준과 본 표준의 비교표

DLTSFx.xx-xx.xxxx/R1	해당 없음	비고

Preface

1 Purpose

The standard is to analyze security threats and clarify security requirements for digital payment systems based on distributed ledger systems in order to provide the basis for development of solutions to meat the requirements.
This standard can be used by organizations which operate digital payment systems based on distributed ledger technologies to identify basic security requirements and develop their unique requirements for the services.

2 Summary

The standard analyze security threats of digital payment systems based on public and private distributed ledger systems model and elicit security threats to address the threats.

3 Relationship to Reference Standards

The standard does not have any reference standard.

목 차

1 적용 범위 ····· x

2 인용 표준 ····· x

3 용어 정의 및 약어 ····· x

4 분산원장기술에 기초한 전자 지불 시스템 모델 ····· x

5 분산원장 기반 전자 지불 시스템에 대한 보안 위협 ····· x

6 분산원장 기반 전자 지불 시스템의 보안 요구사항 ····· x

부록 Ⅰ-1 지식재산권 확약서 정보 ····· x
Ⅰ-2 시험인증 관련 사항 ····· x
Ⅰ-3 본 표준의 연계(family) 표준 ····· x
Ⅰ-4 참고 문헌 ····· x
Ⅰ-5 영문표준 해설서 ····· x
Ⅰ-6 표준의 이력 ····· x

분산원장기술 전자지불 시스템 보안 위협 및 요구사항
Security threats and requirements for digital payment systems based on distributed ledger technologies

1 적용 범위

이 표준은 분산원장기술에 기초한 전자 지불 시스템을 무허가형(permissionless) 및 허가형(permissioned)으로 나누어 개관한다. 또한 분산원장 기반 전자지불시스템에 대한 보안 위협을 전자지불 시스템에 대한 보안 위협 및 분산원장에 대한 보안 위협으로 나누어 분석한다. 이러한 위협에 대한 보안 요구사항을 식별하고 분산원장기반 전자지불시스템의 구성요소 별로 보안 요구사항을 상세화한다. 마지막으로 이러한 요구사항이 무허가형 및 허가형 분산원장 시스템 모델에서 달성될 수 있는 방안을 검토한다.

분산원장기술에 기초한 전자 지불 시스템을 운영하는 기관은 이 표준을 안전한 서비스 제공에 대한 보안 위협 및 보안 요구사항을 확인하고 해당 요구사항을 만족하는 해결책을 개발하는데 활용할 수 있다.

2 인용 표준

TTAK.KO-12.0336 블록체인 용어정의

3 용어 정의

3.1 블록체인 (blockchain)
검증되고 확정된 블록들을 순차적으로 암호학적으로 연결하여 구성되는 분산원장

3.2 분산원장 레코드 (distributed ledger record)
분산원장 내의 한 기록. 블록체인 형 분산원장에서의 레코드는 하나 이상의 거래 데이터와 선행 블록의 해시값을 포함하는 메타데이터가 포함된 블록이다. 비 블록체인 형 분산원장에서의 레코드는 하나의 거래와 하나 이상의 선행 레코드들의 해시값 등의 메타데이터를 포함한다.

3.3 스마트 계약 (smart contract)
분산원장에 기록된 컴퓨터 프로그램으로써 그 실행 결과가 다시 분산원장에 기록되는 프로그램

3.4 분산 애플리케이션 (distributed application, DApp)
분산원장 시스템 상에서 운영되는 애플리케이션. 사용자 인터페이스 및 그에 상응하는 스마트 계약을 포함한다.

3.5 전자 지불 서비스 (digital payment services)
자금을 전자적으로 송금할 수 있게 해 주는 서비스

3.6 무허가형 분산원장 시스템 (permissionless distirubetd ledger systems)
노드 및 사용자가 아무런 허가 없이 분산원장 시스템에 참여할 수 있고 서비스를 이용할 수 있는 시스템. 예를 들어, 비트코인, 이더리움 등이 있다.

3.7 허가형 분산원장 시스템 (permissioned distributed ledger systems)
노드 및 사용자가 분산원장 시스템에 참여 또는 서비스를 이용하기 위하여 허가를 받아야 하는 시스템. 예를 들어, 하이퍼레저 패브릭, R3코다 등이 있다.

3.8 하위 분산원장 시스템 (sub-distributed ledger systems)
허가형 분산원장 시스템에서 다른 노드에는 저장되지 않는 거래를 저장하는 하나 이상의 노드로 구성된 하위 시스템. 비트코인에서 사용되는 라이트닝 체인이 예가 될 수 있다.

3.9 이중 지불 (double spending)
분산원장 내 분기 상에 상충하는 거래가 존재하는 상황

3.10 합의 알고리즘 (consensus algorithm)
분산원장 내 노드들이 상호 통신을 통해 새로운 기록의 공유, 검증 및 추가에 대한 전체의 동의를 이끌어 내는 알고리즘

3.11 시빌 공격 (Sybil attack)
하나의 주체이면서도 다수의 주체인 것으로 가장하여 시스템의 신뢰를 손상시키는 공격

3.12 이기적 채굴 공격 (selfish mining attack)
다른 노드보다 빠르게 블록을 채굴하기 위해 새로운 유효한 블록을 전파하지 않고 해당 블록 이후의 블록을 채굴하는 것. 다른 노드가 새로운 유효한 블록을 채굴한 경우 기존의 유효한 블록을 전파함으로써 다른 노드의 블록을 무효화 한다.

4 약어
이 표준의 목적을 위해 다음의 약어를 사용한다.

DLT Distributed Ledger Technologies

5 분산원장기술에 기초한 전자 지불 시스템 모델

전자 지불 서비스는 자금을 한 계정에서 다른 계정으로 송금하는 서비스다. 전자 지불 시스템은 서비스 제공자의 네트워크 뿐만 아니라 스마트 폰과 같은 이동형 사용자 장비 또는 사용자 컴퓨터를 포함한다.

DLT에 기반한 지불 시스템은 실제로 시장에서 활용되고 있을 뿐만 아니라, 특히 해외 송금의 경우 가장 시간과 비용 측면에서 큰 효과를 가져올 수 있는 사례로 언급되고 있다. 분산원장 시스템은 그 운영 방식에 따라 무허가형(permissionless)과 허가형(permissioned)로 나누어 지는데, 이는 전자 지불 시스템이 제공하는 기능에 영향을 미친다. 4장에서는 이 두 모델을 개관하고, 5장에서는 전자지불 시스템 및 분산원장 시스템에 대한 알려진 보안 위협을 분석한다. 또한 6장에서는 5장의 보안 위협에 대응하기 위한 보안 요구사항을 제시한다.

5.1 무허가형 분산원장 시스템 모델

무허가형 분산원장 시스템에서 사용자는 서비스를 사용하기 위해 어떠한 허가도 필요로 하지 않는다. 사용자는 별도의 등록 절차 없이 자신의 주소, 즉 자신의 공개키(의 해쉬값)으로 거래하게 된다. 이 주소가 계정으로 간주되며, 계정 주소(account address)로 불린다. 송금을 하기 위해 송신자는 수신자의 계정을 알아야 한다. 또한 송신자는 일반적으로 해당 분산원장 시스템이 자금을 저장하거나 송신할 때 사용하는 특정 가치 저장 및 전송용 토큰, 즉 암호화폐를 보유해야 한다.

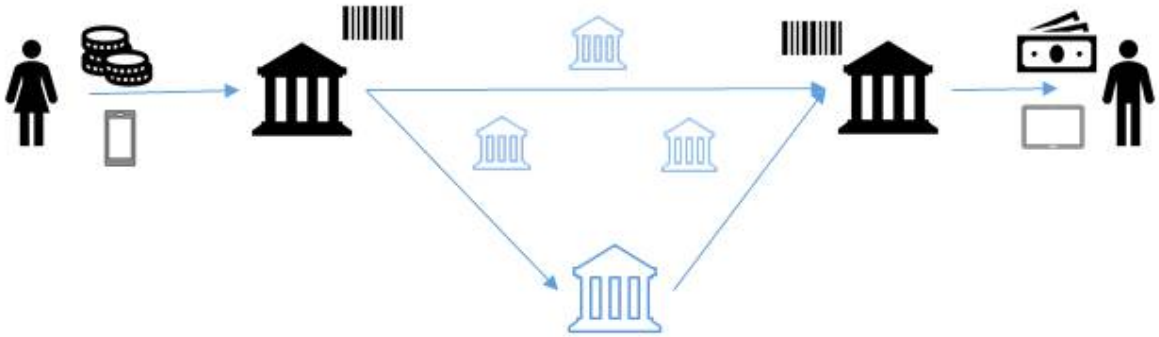
(그림 5-1) 무허가형 분산원장 시스템 모델

특정 금액을 송금하기 위하여 송신자는 자신의 단말기 또는 거래소 등의 보관 기관에 있는 전자 지갑에 접근해야 한다. 송신 트랜잭션은 송신자 계정, 수신자의 계정 및 금액 정보 등에 송신자의 개인 키로 전자 서명되어 분산원장 네트워크에 전파된다.

분산원장 네트워크 내의 각 노드들은 합의 알고리즘에 따라 거래의 유효성을 검증하고 거래 및 자신이 생성한 분산원장 레코드 또는 타 노드로부터 받은, 자신이 합의한 분산원장 레코드를 네트워크에 배포한다. 타 노드로부터 받은 분산원장 레코드들이 합의 알고리즘에 따라 자신이 보유한 레코드보다 더 유효한 것으로 판별된 경우 분산원장 레코드는 갱신될 수 있다.

분산원장 상의 거래는 일반적으로 불변(immutable)이라고 말하지만 이것은 한 거래가 포함된 레코드가 분산원장에 포함된 이후 추가된 레코드들이 충분히 쌓여 더 이상 해당 레코드가 수정되지 않을 것이라고 믿을 수 있을 경우이며 최신의 기록들은 합의 알고리즘에 따라 변경될 수 있다.

5.2 허가형 분산원장 시스템 모델



(그림 5-2) 허가형 분산원장 시스템 모델

허가형 분산원장 시스템에서 노드는 해당 분산원장 시스템에 참여하기 위해 허가를 받아야 한다. 사용자의 경우 해당 분산원장 서비스를 이용하기 위해 등록이 필요한 경우와 그렇지 않은 경우가 있다. 이 표준에서는 무허가형 분산원장 시스템 모델과의 기능 대조를 위해 시스템 사용자 등록을 수행하는 것으로 모델을 구성한다.

실제 이용되고 있는 허가형 분산원장 시스템의 경우 노드는 은행 등 금융기관이 운영하며 사용자는 은행에서 계좌를 개설하고 은행이 제공하는 앱을 이용하여 송금을 수행한다. 동일 통화를 이용하는 경우 이 모델에서 토큰은 필수적이지 않다. 그러나 구현에 따라서는 수수료 지불 및 사용자가 가진 통화가 서로 다를 경우 환전용 토큰, 즉 전자화폐를 사용하는 경우가 있다. 환전 등의 업무를 수행하기 위해서는 관련 정보를 안전한 인터페이스를 통해 연동할 필요가 있다.

사용자는 서비스를 이용하기 위해 허가형 분산원장 시스템에 등록한다. 시스템은 사용자의 신원을 검증하고 계좌를 개설한다. 송신자는 수신자 계좌에 지불을 수행하기 위해 자신의 단말기에 있는 앱에 접근한다.

구현과 정책에 따라 달라질 수 있지만 이 표준에서는 무허가형 분산원장 시스템 모델과의 기능 대조를 위해 암호화 채널 및 하위 분산원장 시스템(sub-distributed ledger system, sub-DLS)을 포함하는 경우를 고려한다.

송신자와 수신자가 같은 하위 분산원장 시스템에 등록되어 있는 경우 거래는 해당 하위 분산원장 시스템에만 전송된다. 송신자와 수신자가 서로 다른 하위 분산원장 시스템에

등록되어 있는 경우 송신자의 하위 분산원장 시스템은 송진자의 하위 분산원장 시스템에 거래를 전송한다. 이 거래는 상위 분산원장 시스템 또는 제3의 연결점(또는 하위 분산원장 시스템)을 통해 기록된다. 하위 분산원장 시스템 또는 별도의 분산원장 시스템과의 연결을 위해서는 안전한 인터페이스를 통해 동기화할 필요가 있다

5.3 분산원장 기반 전자 지불 시스템 구성 요소

상기 두 모델에서 보듯 분산원장 기반 전자 지불 시스템은 여러 요소로 구성된다. 이러한 구성 요소를 파악하는 것은 다음 장에서 나타나는 보안 위협이 어느 요소에 영향을 미치며 이에 대한 요구사항을 어느 요소에서 만족해야 할지를 결정하는데 필요하다. 분산원장 기반 전자 지불 시스템의 구성 요소는 다음과 같다.

- 이용자 단말
- DLT 노드
- 분산원장 시스템 관리
- 연계 인터페이스

이들의 기능은 다음과 같다.

- 이용자 단말에서는 분산 애플리케이션(DApp)을 설치, 수행한다. 이러한 DApp에는 이용자의 공개키 쌍을 생성, 보관 및 이용하는 전자 지갑이 대표적인 예가 될 수 있다. 또한 분산원장에 지불 거래를 요청하거나 거래 기록을 검색하기 위한 기능도 포함된다. 분산 애플리케이션은 분산원장에 기록된 스마트 컨트랙트를 호출할 수 있다.

- DLT 노드는 거래의 공유·검증, 분산원장 기록의 생성, 공유, 합의, 저장, 스마트 계약 실행 및 상태 저장 등 분산원장 시스템의 핵심 기능을 수행한다. 무허가형 분산원장 시스템에서는 누구나 노드를 운영할 수 있으나 허가형 분산원장 시스템에서는 승인된 기관만이 노드를 운영한다. 노드는 합의 등을 위해 자신의 공개키 쌍을 생성, 보관 및 사용한다. 허가형 분산원장 시스템에서는 정책에 따라 노드들이 검증, 순서 결정 등 서로 다른 기능을 수행할 수 있다. 또한 분산원장 시스템 기능을 수행하는 별도의 시스템 또는 노드가 DLT 네트워크 상에 존재할 수 있다.

- 분산원장 시스템 관리는 분산원장 시스템 전체에 걸친 관리 기능이다. 무허가형 분산원장 시스템에서 이 기능은 프로토콜에 내재되어 각각의 노드 내에서 수행된다. 프로토콜의 변경은 분산원장 시스템의 관리를 변경할 수 있으며, 각각의 노드가 변경된 프로토콜을 채택함으로써 암묵적으로 관리에 동의하게 된다. 변경된 프로토콜이 분산원장 네트워크의 전체 노드에 채택되지 않는다면 분산원장의 분기가 발생할 수 있다. 한편 허가형 분산원장에서는 노드 관리, 정책 관리 등 다양한 관리 기능이 존재할 수 있으며 이를 수행하기 위한 별도의 시스템 또는 노드가 존재할 수 있다.

- 연계 인터페이스는 분산원장 시스템과 비 분산원장 시스템 간 또는 분산원장 시스템과 타 분산원장 시스템 간의 연계를 제공한다. 이들은 별도의 구성요소로 존재할 수 있다. 분산원장 시스템 내의 데이터의 무결성을 유지하기 위하여 이러한 연계 인터페이스는 신뢰할 수 있는 타 시스템 또는 타 분산원장 만을 연계하여야 하며, 신뢰할 수 있는 정보 만을 제공해야 한다. 분산원장 간 정보의 이동을 안전하게 관리하기 위하여 동기화 기능을 제공한다.

6 분산원장 기반 전자 지불 시스템에 대한 보안 위협

분산원장 기반 전자지불시스템에 대한 알려진 보안 위협은 전자지불 시스템에 대한 보안 위협, 분산원장에 대한 보안 위협, 그리고 분산원장 기반의 전자지불로 인해 발생할 수 있는 위협으로 나누어 볼 수 있다.

이 외에도 노드가 운영되는 시스템에 대한 전통적인 외부자 해킹, 내부자 공격 등이 발생할 수 있으나 이는 이 표준의 범위에서 제외한다.

6.1 일반적인 전자 지불 서비스에 대한 보안 위협

일반적인 전자 지불 서비스에 대한 보안 위협은 많이 알려져 있다. 다음의 <표 6-1>은 전자 지불 환경에서의 일반적인 지불 위협을 제시한다.

<표 6-1> 전자지불 환경에서의 지불 부정 보안 위협

위협 유형	전통적 방식	전자지불 환경의 특성
위조 계정 개설	물리적 신분증 절도, 신분증 위조	신분증의 위조가 더 용이
위조 거래	물리적인 지불 증명 절도, 서명 위조	원격 거래 상의 지불 메커니즘 보호 수단이 더 적어져 추가 보안 대책이 필요함 온라인 또는 저장된 크리덴셜 해킹, PIN 절도 등이 더 용이
사기	구두 사기, 현금 수금	SMS 및 E-mail 스팸이 더 많은 대상에게 전달, 전자송금을 통해 더 큰 규모의 자금 모금 용이
시스템적 부정	백오피스 지점 계좌 조작	대규모 관리 시스템의 복잡성이 규제 통제를 어렵게 할 수 있음
돈세탁/ 범죄 자금 조달	현금 및 은행 계좌 송금	대규모의 소액 송금이 가능하여 감독기관이 발견하기 어려움

6.2 일반적인 분산원장 서비스에 대한 보안 위협

일반적인 분산원장 서비스에 대한 보안 위협은 다음의 <표 6-2>에서 설명한다.

<표 6-2> 일반적인 분산원장 서비스에 대한 보안 위협

위협 유형	발생 방식	위협의 영향
eclipse 공격	P2P 프로토콜을 사용하는 공격 대상 노드의 주소 테이블 손상	대상 노드가 해당 DLT 네트워크에서 분리, 이중지불 등
DDoS 공격	실제로는 의미 없는 다량의 트랜잭션을 생성 기록 요청 거래가 없거나 스팸 거래로 이루어진 블럭을 전송	실제 중요한 트랜잭션이 적시 처리되지 못함
개인키 노출	사용자의 장비에 악성코드 감염 또는 키 저장소 약점을 이용한 키 절도, 출력된 개인키 절도	메시지 위조
개인키 분실	백업 없이 키 저장 장비 손상, 키 사용을 위한 패스워드 등 분실, 출력된 개인키 분실	해당 키에 상응하는 자원에 대한 통제 및 권리의 주장 불가
암호 알고리즘 공격	알고리즘 취약성을 이용한 키 획득, 양자 암호 분석을 통한 키 획득, 동일 해시 값 데이터 조작	키 획득 또는 데이터 위조
합의 알고리즘 공격	51% 공격 타임스탬프 조작 공격 이기적 채굴 공격 시빌 공격	새로운 분기(fork)로 기존 메인 체인의 블록을 교체
스마트 컨트랙트 공격	예외 처리 미흡 타임스탬프 검증 미흡 메모리 오염 공격 스마트 컨트랙트 실행환경 공격	실제 실행되어서는 안될 상황에서의 코드 실행
개인정보 유출	블록체인 상에 기록된 개인정보가 권한없는 자에게 유출	개인정보 도난 및 오남용

6.3 분산원장에 기반한 전자지불 서비스에 대한 보안 위협

분산원장 기반의 전자지불 서비스에 대한 대표적인 보안 위협의 예로는 이중 지불이 있다. 하나의 거래가 제출되어 전체 분산원장에서 최종적으로 확정되기 까지는 전체 노드

가 합의에 도달하기 위한 시간이 필요하므로 하나의 자산에 대해 서로 다른 거래를 네트워크 상의 서로 다른 노드에 제출하여 일부 노드의 합의를 얻음으로써 상충하는 두 거래가 분산원장 네트워크 상에 존재하는 것이 가능하다. 거래가 확정되지 않은 상태에서 한 거래의 상대 당사자가 지불이 이루어졌다고 믿고 대가를 제공하였으나 이후 전체 네트워크가 합의에 도달했을 때 그 거래가 거부되었다면 그 당사자는 손실을 보게 된다.

7 분산원장 기반 전자 지불 시스템에 대한 보안 요구사항

7.1 절에서는 6장에서 분석한 보안 위협에 대한 보안 요구사항을 표로 제시한다. 7.2절 이하에서는 해당 보안 요구사항을 분산원장 기반 전자 지불 시스템의 각 구성요소에 대하여 상세화하여 제시한다. 구성요소의 구분은 5.3절에서 제시된 4개 구성요소를 따르되 스마트 컨트랙트의 보안 요구사항은 개발, 실행 및 관리에 관한 부분이 포함되어 있으며 연계 인터페이스와도 관련되어 있으므로 별도 항목으로 구분하여 제시하였다.

7.1 보안 위협 대비 보안 요구사항

<표 7-1> 보안 위협 대비 보안 요구사항

보안 위협	보안 요구사항	비고
위조 계정 개설	정당한 사용자인지 인증해야 한다.	7.2.3, 7.4.3
위조 거래	안전한 암호 알고리즘을 사용해야 한다. 키에 대한 접근을 통제해야 한다.	7.2.5, 7.4.2
사기	부정 및 사기를 방지해야 한다.	7.4.6
시스템적 부정	프로그램의 위변조를 통제해야 한다	7.2.4, 7.3.4, 7.5.2, 7.3.3, 7.3.4
돈세탁/ 범죄 자금 조달	불법행위를 방지해야 한다.	7.4.6
eclipse 공격	정당한 노드인지 인증해야 한다.	7.3.1
DDoS 공격	비정상 거래 및 블록을 검증해야 한다.	7.3.2
개인키 노출	키에 대한 접근을 통제해야 한다.	7.2.5
개인키 분실	키 등 중요 데이터를 백업해야 한다	7.2.2
암호 알고리즘 공격	안전한 암호 알고리즘을 사용해야 한다. 신규 취약점 발생 시 안전한 알고리즘으로 변환할 수 있어야 한다.	7.4.2, 7.4.11
합의 알고리즘 공격	정당한 노드인지 인증해야 한다. 정족수 기준을 마련해야 한다.	7.3.1, 7.4.4 7.4.10

스마트 컨트랙트 공격	스마트 컨트랙트 코드를 검증해야 한다.	7.5.1, 7.5.3, 7.5.4
개인정보 유출	개인정보를 분산원장에 기록하지 말아야 한다.	7.4.9
이중 지불	거래 확정 기준을 마련해야 한다	7.2.6

7.2 사용자 단말 장비에 대한 보안 요구사항

7.2.1. 장비는 원격 비활성화 기능 등을 이용하여 도난/분실 시에도 데이터를 보호할 수 있어야 한다.
7.2.2. 개인 키 등 장비 내의 중요 데이터에 대한 백업이 이루어져야 한다.
7.2.3. 장비 사용 시 정당한 사용자인지 여부를 인증해야 한다.
7.2.4. 앱 구동 시 장비 및 앱 무결성을 확인해야 한다
7.2.5. 키를 안전한 방식으로 생성, 저장, 이용 및 파기해야 한다.
7.2.6. 합의 알고리즘 특성에 따른 거래 확정 기준(예, 거래 포함 블록 이후 6개 이상의 블록 추가 시점 등)을 마련하고 확정된 거래를 확인해야 한다.

7.3 노드에 대한 보안 요구사항

7.3.1. 통신하고 있는 노드를 확인할 수 있는 방법을 마련해야 한다
7.3.2. 비정상 거래 및 블록을 검증해야 한다
7.3.3. 노드 플랫폼 외의 불필요한 서비스를 운영해서는 안된다.
7.3.4. 노드 플랫폼 및 연계 인터페이스의 보안을 정기적으로 확인하여야 한다.

7.4 분산원장 시스템 관리에 대한 보안 요구사항

7.4.1. 분산원장 시스템 관리를 위한 정책 수립, 의사결정 구조 수립, 책임자 지정 등을 포함하는 프레임워크를 수립해야 한다.
7.4.2. 안전한 암호 알고리즘 및 적절한 길이의 키를 사용해야 한다.
7.4.3. 사용자 및 참여자에 대한 가입 허가 기준을 수립하고 이행해야 한다
7.4.4. 노드에 대한 네트워크 가입 기준을 수립하고 이행해야 한다.
7.4.5. 계정 개설 시 실 사용자를 확인해야 한다.
7.4.6. 부정 및 불법행위, 사기를 방지하기 위해 데이터 흐름을 분석하여 이상거래를 확인해야 한다.
7.4.7. 장비 이상, 네트워크 해킹, 개인정보 침해, 불법행위 발생 등 사고에 대한 대응 절차를 마련하고 이행해야 한다.
7.4.8. 암호화, 하위 분산원장 등 필요시 데이터 기밀성을 제공할 수 있어야 한다.
7.4.9. 개인정보를 분산원장에 기록하지 않도록 방안을 수립하고 이행해야 한다.

7.4.10. 합의 알고리즘에 따라 정족수 기준을 마련하고 네트워크 모니터링을 통해 노드 현황을 관리해야 한다.
7.4.11. 시스템 관리 기능의 자체 안전성을 포함하여 분산원장 기술 및 운영 전반에 걸친 취약점을 모니터링하고 대응 관리하여야 한다.

7.5 스마트 컨트랙트에 대한 보안 요구사항

7.5.1. 등록 전 스마트 컨트랙트 코드를 검증해야 한다.
7.5.2. 스마트 컨트랙트 등록 권한을 제한해야 한다.
7.5.3. 실행 시 스마트 컨트랙트 실행환경 보안, 실행 권한 및 자원 확인, 무한 반복 방지 등 스마트 컨트랙트 실행 조건을 검증해야 한다.
7.5.4. 분산원장 외부의 정보를 이용할 경우 안전한 연계 인터페이스를 통해야 한다.
7.5.5. 스마트 컨트랙트 취약점에 따른 위험을 지속적으로 관리해야 한다.

7.6 연계 인터페이스에 대한 보안 요구사항

7.6.1. 연계 정책 및 기준에 따라 시스템 간 정보의 흐름을 통제해야 한다.
7.6.2. 신뢰할 수 있는 정확한 정보를 적시에 제공해야 한다.
7.6.3. 두 시스템 간 연계되는 정보를 동기화해야 한다.
7.6.4. 기밀성이 요구되는 데이터가 유출되지 않도록 해야 한다

8 분산원장 시스템 모델에 따른 보안 위협 대응 방안

<표 7-1>의 위협들은 각각 개별적으로 적용될 수도 있으나 서로 영향을 미치거나 시나리오 형태로 연계될 수 있다. 또한 시스템의 취약성은 구체적인 구현 방법에 따라 다양하지만, 기반이 되는 모델에 따라 기본적인 대응 방법이 달라질 수 있다. 예를 들어 무허가형 분산원장 시스템 모델에서는 이용자 신원 확인에 대한 보안 요구사항 및 금융 규제 관련 요구사항을 만족하기 어렵다. 그러나 허가형 분산원장 시스템 모델에서는 기본적인 대응이 가능하다. 또한 두 모델에서 모두 대응 가능한 위협에 대해서도 대응하는 방법이 달라질 수 있다. <표 8-1>은 각 위협에 대해 무허가형과 허가형에서 어떤 방식으로 대응 가능한 지를 설명하고 있다.

<표 8-1> 분산원장기반 전자지불 시스템의 보안 위협에 대한 대응 방안

위협	무허가형	허가형
위조 계정 개설	계정 주소 외 소유자 확인불가	사용자 등록 프로세스 강화
위조 거래/사기	구제 방안 없음	조직 간 합의 또는 법집행기관의 개입에 의한 보상 거래 수행

시스템적 부정	프로토콜 변경(분기)	중앙 모니터링 및 프로토콜 변경
돈세탁/범죄 자금 조달	시스템 외적으로 범죄 자금 계정 이동 추적 및 현금화 시 각국 법률에 기초하여 처리	관리 시스템에서 돈세탁 방지, 불법자금 방지를 위한 검출 및 추적 적용
Eclips 공격	주소 처리 프로세스 강화	노드 관리 프로세스 강화
DDoS 공격	거래(블록) 검증 알고리즘 강화	노드 관리 프로세스 및 거래(블록) 검증 알고리즘 강화
개인 키 노출/분실	키 관리 프로세스 강화	키 관리 프로세스 강화
암호 알고리즘 공격	프로토콜 변경	중앙 정책 변경 및 프로토콜 변경
합의 알고리즘 공격	안전한 합의 알고리즘 선정 (대체로 나카모토 컨센서스의 일종으로 51% 공격 가능)	안전한 합의 알고리즘 선정 및 참여자 관리 (대체로 비잔틴 컨센서스의 일종으로 정족수 공격 가능하나 참여자 검증 및 노드 보안 수준 관리로 가능성 낮음)
스마트 컨트랙트 공격	패치, 프로토콜 변경 등	등록 및 권한 관리
개인정보 유출	사용자 스스로 개인정보를 분산원장에 기록 하지 말아야 하며, 개인정보를 기록한 경우 보호 방법이 거의 없음	정책 수립 및 모니터링 조직 간 합의 또는 법집행기관의 개입에 의한 기록 변경
이중 지불	알려진 거래 확정 기준에 따라 이용자가 각자 대응	조직 간 합의 또는 법집행기관의 개입에 의한 보상 거래 수행

상기 표에서 보이는 바와 같이 허가형 분산원장 시스템에서는 대부분의 위협에 대하여 세부적인 보안 정책 수립 및 이행 등을 통한 대응이 가능하지만 무허가형에서는 구제 및 대응이 어려운 보안 위협들이 존재한다. 전자지불 거래의 안전 이용을 위해서는 허가형 모델을 기반으로 하여 보안 요구사항을 만족할 수 있는 더 구체적인 보안 통제를 개발, 구현할 필요가 있다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

Ⅰ-1.1 지식재산권 확약서

해당사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, DLTSF 웹사이트에서 확인하시기 바랍니다.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

Ⅰ-2.1 시험인증 대상 여부

해당사항 없음

Ⅰ-2.2 시험표준 제정 현황

해당사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

Ⅰ-3.1 블록체인 용어 정의

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

[1] ITU-T Technical Report *Digital Financial Services(DFS) Glossary.* https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201701/*ITU_FGDFS_DFS-Glossary.pdf*

[2] ITU-T Technical Report *Security Aspect of Digital Financial Services(DFS)* https://www.itu.int/en/ITU-T/studygroups/2017-2020/09/Documents/ITU_FGDFS_SecurityReport.pdf

[3] ITU-T Technical Report *Distributed Ledger Technologies and Financial inclusion* https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/201703/ITU_FGDFS_Report-on-DLT-and-Financial-Inclusion.pdf

[4] ITU-T Technical Report *Digital Financial Services Ecosystem* https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/FINAL%20ENDORSED%20ITU%20DFS%20Introduction%20Ecosystem%2028%20April%202016_formatted%20AM.pdf

[5] ENISA, Distributed ledger technology & cybersecurity, 2016.

[6] EBA, Final guidelines on the security of internet payments, 2014

[7] ITU-T SG 17 X.sct-dlt, Security threats of distributed ledger technology, https://www.itu.int/ITU-T/workprog/wp_item.aspx?isn=14373

부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판	2018.XX.XX	제정 DLTSFx.xx-xx.xxxx	-	기반 분과