TTA Standard

정보통신단체표준(국문표준)

TTAK.KO-12.0374

제정일 2021.12.08.

(2025 확인)

분산원장기술 기반 가상자산 송금 이용자 신원 확인 서비스 모델

Virtual Asset Transfer Customer Identification Service Model Based On Distributed Ledger Technology

TTA 한국정보통신기술협회
Telecommunications Technology Association

TTAStandard

정보통신단체표준(국문표준)

TTAK.KO-12.0374 제정일: 2021 년 12 월 8 일

분산원장기술 기반 가상자산 송금 이용자 신원 확인 서비스 모델

Virtual Asset Transfer Customer Identification Service Model Based On Distributed Ledger Technology

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 개인정보보호/ID관리, 블록체인 보안(PG502)

표준안 심의 위원회 정보보호기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위
표준(과제) 제안	박근덕	서울외국어대학원대학교	교수	PG502 위원
표준 초안 에디터	박근덕	서울외국어대학원대학교	교수	PG502 위원
	염흥열	순천향대학교	교수	PG502 위원
사무국 담당	이강해	한국정보통신기술협회	단장	-
	박수정	한국정보통신기술협회	책임	

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. 준용표준인 경우 해당 표준화기구 또는 단체의 웹사이트에서 이를 확인해야 합니다.
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 : 2021. 12. 8.

서 문

1 표준의 목적

이 표준의 목적은 분산원장기술 기반 가상자산 송금 이용자 신원 확인 서비스 모델을 정의함에 있다. 최근 블록체인 기반 가상자산(암호화폐)을 활용한 국경 간 송금(이전)이 증가하고 있는 추세이다. 그러나 블록체인의 익명성에 기인하여 가상자산사업자는 이용자(송금인 및 수취인)의 신원을 확인할 수 없기 때문에 자금세탁 관련 문제점이 존재한다. 이러한 문제점을 해결하기 위하여 가상자산사업자는 자금세탁방지를 위한 고객확인의무(CDD) 및 신원 정보 제공 규칙(예: 트래블룰, travel rule)을 준수할 수 있는 서비스 모델이 필요하다. 가상자산사업자는 신원관리사업자가 참여하는 본 서비스 모델을 통하여 이용자의 개인정보를 포함한 신원 정보를 안전하게 확인 및 보관할 수 있다.

2 주요 내용 요약

이 표준은 자금세탁방지 및 개인정보보호 관련 법규정의 분석을 통하여 가상자산 관련 자금세탁방지를 위한 이용자 신원 확인 및 신원 정보 제공, 개인정보 파기 및 가명처리 등 요구사항을 식별하고, 가상자산사업자가 이용자(송금인 및 수취인)의 신원 정보를 확인할 수 있는 분산원장기술 기반 이용자 신원 확인 서비스 모델과 데이터 규격을 정의한다. 또한 이용자 신원 확인 서비스에 대한 보안 위협을 식별하고 그에 대응하는 보안 요구사항을 기술한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

해당 사항 없음

3.2 인용 표준과 본 표준의 비교표

해당 사항 없음

Preface

1 Purpose

The purpose of this standard is to define virtual asset transfer customer identification service model based on distributed ledger technology (DLT). Recently, cross-border transfers using blockchain-based virtual assets (i.e., cryptocurrencies) have been increasing. However, due to the anonymity of the blockchain, there is a problem related to money laundering because the virtual asset service provider (VASP) cannot identify the originator and the beneficiary. To solve this problem, the VASPs need a service model that can implement the customer due diligence (CDD) and rule to provide customer identity information (e.g., travel rule) for anti-money laundering (AML). The VASPs can securely verify and store customer identity information including PII (personally identifiable information) using this service model which includes identity service providers (IDSPs).

2 Summary

This standard should identify requirements such as CDD and the travel rule to implement AML and pseudonymization of PII through analysis of AML laws and guidelines related to virtual assets and laws related to personal data protection, and should define a customer identification service model based on DLT and data formats that enable VASPs to verify identity information of the originators and beneficiaries. And also this standard should identify security threats to the service and specify security requirements against the identified security threats.

3 Relationship to Reference Standards

None

목 차

분산원장기술 기반 가상자산 송금 이용자 신원 확인 서비스 모델 (Virtual Asset Transfer Customer Identification Service Model Based On Distributed Ledger Technology)

1 적용 범위

본 표준은 가상자산 송금 시 이용자(송금인 및 수취인)의 신원을 확인할 수 있는 서비스 모델과 데이터 규격을 정의한다. 또한 이용자 신원 확인 서비스에 대한 보안 위협을 식별하고 그에 대응하는 보안 요구사항을 기술한다.

2 인용 표준

해당 사항 없음

3 용어 정의

3.1 가상자산 (VA, virtual asset)

경제적 가치를 지닌 것으로서 전자적으로 거래 또는 이전될 수 있는 전자적 증표(그에 관한 일체의 권리를 포함한다)를 말한다. 다만, 다음 각 목의 어느 하나에 해당하는 것은 제외한다. 가. 화폐·재화·용역 등으로 교환될 수 없는 전자적 증표 또는 그 증표에 관한 정보로서 발행인이 사용처와 그 용도를 제한한 것 나. 「게임산업진흥에 관한 법률」 제32조제1항제7호에 따른 게임물의 이용을 통하여 획득한 유·무형의 결과물 다. 「전자금융거래법」 제2조제14호에 따른 선불전자지급수단 및 같은 조 제15호에 따른 전자화폐 라. 「주식·사채 등의 전자등록에 관한 법률」 제2조제4호에 따른 전자등록주식등 마. 「전자어음의 발행 및 유통에 관한 법률」 제2조제2호에 따른 전자어음 바. 「상법」 제862조에 따른 전자선하증권 사. 거래의 형태와 특성을 고려하여 대통령령으로 정하는 것.

※ 참고: 암호화폐(예: 비트코인, 이더리움, 리플 등)가 가상자산에 해당됨

3.2 가상자산사업자 (VASP, virtual asset service provider)

가상자산과 관련하여 다음 1)부터 6)까지의 어느 하나에 해당하는 행위를 영업으로 하는 자 1) 가상자산을 매도, 매수하는 행위 2) 가상자산을 다른 가상자산과 교환하는 행위 3) 가상자산을 이전하는 행위 중 대통령령으로 정하는 행위 4) 가상자산을 보관 또는 관리하는 행위 5) 1) 및 2)의 행위를 중개, 알선하거나 대행하는 행위 6) 그 밖에 가상자산과 관련하여 자금세탁행위와 공중협박자금조달행위에 이용될 가능성이 높은 것으로서 대통령령으로 정하는 행위.

※ 참고: 암호화폐 거래소, 보관 사업자, 지갑 사업자 등이 가상자산사업자에 해당됨

[출처(3.1~3.2)] 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」

3.3 신원관리사업자 (IDSP, identity service provider)

정보주체(개인 또는 법인)의 신원을 검증하고 디지털 신원(Identity)을 발급, 이용, 갱신, 파기하는 것을 영업으로 하는 개인 또는 법인.

※ 참고: 본인확인기관, 전자서명인증사업자 등이 신원관리사업자에 해당됨

3.4 개인정보 (PII, personally identifiable information)

살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다. 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다. 다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다).

3.5 가명처리 (pseudonymization)

개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

[출처(3.4~3.5)] 「개인정보 보호법」

3.6 온체인 (on-chain)

블록체인 내에서 이루어진 프로세스 혹은 블록체인 내의 데이터 등을 수식할 때 사용된다.

3.7 오프체인 (off-chain)

블록체인 외에서 이루어진 프로세스 혹은 블록체인 외부에 저장된 데이터 등을 수식할 때 사용된다.

[출처(3.6~3.7)] TTAK.KO-12.0336 블록체인 용어정의

3.8 허가형 분산원장시스템 (permissioned DLT system)

노드를 유지하고 운영하기 위해 권한이 필요한 분산원장시스템 (distributed ledger system in which permissions are required to maintain and operate a node).

3.9 비공개 분산원장시스템 (private DLT system)

제한된 DLT 사용자 그룹만 사용할 수 있는 분산원장시스템 (a distributed ledger technology (DLT) system which is accessible for use only to a limited group of DLT users).

[출처(3.8~3.9)] ITU-T X.1400 분산원장기술 용어 정의 (terms and definitions for distributed ledger technology)

4 약어

AML	anti-money laundering
CDD	customer due diligence
DLT	distributed ledger technology
IDSP	identity service provider
PKI	public key infrastructure
VASP	virtual asset service provider

5 가상자산 이용자 신원 정보 처리 관련 법규정에 근거한 요구사항

5.1 가상자산 이용자 신원 확인 및 신원 정보 제공

본 절에서는 국제자금세탁방지기구(FATF, Financial Action Task Force)의 지침을 반영하여 개정된 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」 및 「특정 금융거래정보 보고 및 감독규정」에 근거하여 가상자산 관련 자금세탁방지를 위한 이용자 신원 확인 및 신원 정보 제공 요구사항을 분석한다. 가상자산사업자는 본 요구사항을 준수하여야 하고, 제6장에서 제안한 서비스 모델을 통하여 가상자산 송금 시 이용자(송금인 및 수취인)의 신원 정보를 확인 및 제공할 수 있다.

- **법 제5조의2(금융회사등의 고객 확인의무)** ① 금융회사등은 금융거래등을 이용한 자금세탁행위 및 공중협박자금조달행위를 방지하기 위하여 합당한 주의(注意)로서 다음 각 호의 구분에 따른 조치를 하여야 한다. 이 경우 금융회사등은 이를 위한 업무 지침을 작성하고 운용하여야 한다.

  1. 고객이 계좌를 신규로 개설하거나 대통령령으로 정하는 금액 이상으로 일회성 금융거래등을 하는 경우: 다음 각 목의 사항을 확인

  가. 대통령령으로 정하는 고객의 신원에 관한 사항

  나. 고객을 최종적으로 지배하거나 통제하는 자연인(이하 이 조에서 “실제 소유자”라 한다)에 관한 사항. 다만, 고객이 법인 또는 단체인 경우에는 대통령령으로 정하는 사항

  2. 고객이 실제 소유자인지 여부가 의심되는 등 고객이 자금세탁행위나 공중협박자금조달행위를 할 우려가 있는 경우: 다음 각 목의 사항을 확인

  가. 제1호 각 목의 사항

  나. 금융거래등의 목적과 거래자금의 원천 등 금융정보분석원장이 정하여 고시하는 사항(금융회사등이 자금세탁행위나 공중협박자금조달행위의 위험성에 비례하여 합리적으로 가능하다고 판단하는 범위에 한정한다)
- **법 제5조의3(전신송금 시 정보제공)** ① 금융회사등은 송금인이 전신송금(電信送金: 송금인의 계좌보유 여부를 불문하고 금융회사등을 이용하여 국내외의 다른 금융회사등으로 자금을 이체하는 서비스를 말한다)의 방법으로 500만원의 범위에서 대통령령으로 정하는 금액 이상을 송금하는 경우에는 다음 각 호의 구분에 따라 송금인 및 수취인에 관한 정보를 송금받는 금융회사등(이하 “수취 금융회사”라 한다)에 제공하여야 한다.

  1. 국내송금

  가. 송금인의 성명(법인인 경우에는 법인의 명칭을 말한다. 이하 같다)

  나. 송금인의 계좌번호(계좌번호가 없는 경우에는 참조 가능한 번호를 말한다. 이하 같

다)

다. 수취인의 성명 및 계좌번호

2. 해외송금

가. 송금인의 성명

나. 송금인의 계좌번호

다. 송금인의 주소 또는 주민등록번호(법인인 경우에는 법인등록번호, 외국인인 경우에는 여권번호 또는 외국인등록번호를 말한다)

라. 수취인의 성명 및 계좌번호

- **시행령 제10조의3(일회성 금융거래등의 금액)** ①법 제5조의2제1항제1호 각 목 외의 부분에서 “대통령령으로 정하는 금액”이란 다음 각 호의 구분에 따른 금액을 말한다.

  1의2. 법 제2조제2호라목에 따른 가상자산거래(이하 “가상자산거래”라 한다)의 경우: 1백만원에 상당하는 가상자산의 금액. 이 경우 가상자산의 현금 환산 기준은 금융정보분석원장이 정하여 고시한다.

- **시행령 제10조의4(고객의 신원에 관한 사항)** 법 제5조의2제1항제1호가목에서 “대통령령으로 정하는 고객의 신원에 관한 사항”이란 다음 각 호의 구분에 따른 사항을 말한다.

  1. 개인(다른 개인, 법인 또는 그 밖의 단체를 위한 것임을 표시하여 금융거래등을 하는 자를 포함한다)의 경우: 실지명의(전자금융거래의 경우 금융정보분석원장이 정하여 고시하는 고객에 대해서는 실지명의 대신 성명, 생년월일 및 성별 등 금융정보분석원장이 정하여 고시하는 사항을 말한다), 주소, 연락처(전화번호 및 전자우편주소를 말한다. 이하 같다)

  2. 영리법인의 경우 : 실지명의, 업종, 본점 및 사업장의 소재지, 연락처, 대표자의 성명, 생년월일 및 국적

  3. 비영리법인 그 밖의 단체의 경우 : 실지명의, 설립목적, 주된 사무소의 소재지, 연락처, 대표자의 성명, 생년월일 및 국적

  4. 외국인 및 외국단체의 경우 : 제1호 내지 제3호의 규정에 의한 분류에 따른 각 해당 사항, 국적, 국내의 거소 또는 사무소의 소재지

- **시행령 제10조의8(정보제공대상 전신송금 기준금액)** 법 제5조의3제1항 각 호 외의 부분에서 “대통령령으로 정하는 금액”이란 다음 각 호의 구분에 따른 금액을 초과하는 금액을 말한다.

  1. 국내송금의 경우: 원화 1백만원 또는 그에 상당하는 다른 통화로 표시된 금액

  2. 해외송금의 경우: 1천 미합중국달러 또는 그에 상당하는 다른 통화로 표시된 금액

- **감독규정 제26조(가상자산의 가격 산정 방식)** ① 영 제10조의3제1항제1호의2에서 "가상자산의 현금 환산 기준"이란 가상자산의 매매·교환 거래체결 시점 또는 법 제2조제1호하목에 따른 가상자산사업자(이하 "가상자산사업자"라 한다)가 가상자산의 이전을 요청받거나 가상자산을 이전받은 시점에서 가상자산사업자가 표시하는 가상자산의 가액을 적용하여 원화로 환산하는 것을 말한다.

특히, 「특정 금융거래정보의 보고 및 이용 등에 관한 법률」제5조의3(전신송금 시 정보제공)은 트래블룰(travel rule)로도 잘 알려져 있다.

5.2 개인정보 파기 및 가명처리

본 절에서는 「개인정보 보호법」에 근거하여 가상자산 송금 이용자(송금인 및 수취인)의 개인정보 파기 및 가명처리 요구사항을 분석한다. 가상자산사업자는 본 요구사항을 준수하여야 하고, 제6장에서 제안한 서비스 모델을 통하여 가상자산 이용자의 신원 정보에 포함된 개인정보를 완전 삭제, 가명처리 등의 방법으로 보호할 수 있다.

- **법 제21조(개인정보의 파기)** ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.
  ② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.
  ③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.
  ④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

- **법 제28조의2(가명정보의 처리 등)** ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.
  ② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

- **법 제28조의4(가명정보에 대한 안전조치의무 등)** ① 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.
  ② 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.

- **법 제28조의5(가명정보 처리 시 금지의무 등)** ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.
  ② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.

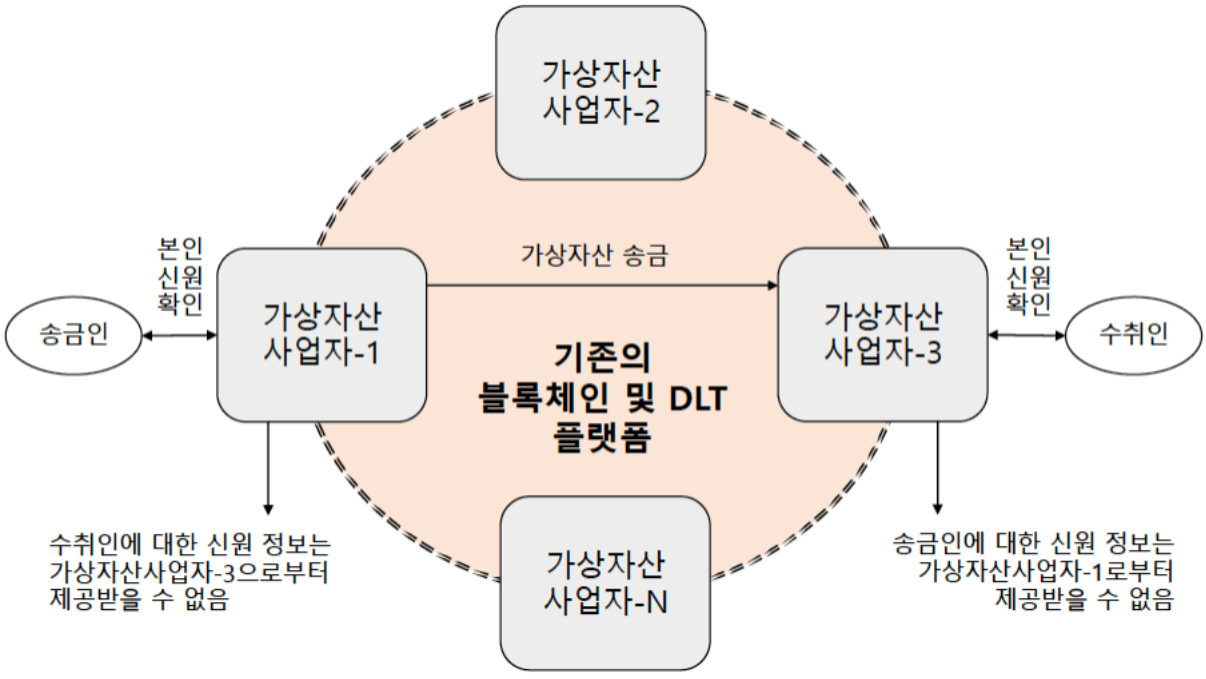
- **시행령 제16조(개인정보의 파기방법)** ①개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.
  1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
  2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각
  ② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 보호위원회가 정하여 고시한다.

- **시행령 제29조의5(가명정보에 대한 안전성 확보 조치)** ① 개인정보처리자는 법 제28조의4제1항에 따라 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보(이하 이 조에서 “추가정보”라 한다)에 대하여 다음 각 호의 안전성 확보 조치를 해야 한다.
  1. 제30조 또는 제48조의2에 따른 안전성 확보 조치
  2. 가명정보와 추가정보의 분리 보관. 다만, 추가정보가 불필요한 경우에는 추가정보를 파기해야 한다.
  3. 가명정보와 추가정보에 대한 접근 권한의 분리. 다만, 「소상공인기본법」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다.
  ② 법 제28조의4제2항에서 “대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다.
  1. 가명정보 처리의 목적
  2. 가명처리한 개인정보의 항목
  3. 가명정보의 이용내역
  4. 제3자 제공 시 제공받는 자
  5. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항

6 가상자산 송금 이용자 신원 확인 서비스 모델

6.1 가상자산 송금 시 익명성 문제점

가상자산사업자(VASP)는 가상자산 송금(이전) 시 자금세탁방지(AML)를 위하여 고객확인의무(CDD) 및 신원 정보 제공(예: 트래블룰)을 준수해야 하지만, 기존의 블록체인 및 분산원장기술(DLT) 플랫폼 환경에서 가상자산을 송금할 때 고객(이용자) 신원정보를 확인할 수 없는 문제가 있다. 이러한 문제는 기존 블록체인 및 DLT 플랫폼의 익명성에 기인한다. 예를 들어 최근 잘 알려져 있고 널리 사용되는 DLT 플랫폼인 하이퍼레저 패브릭(Hyperledger Fabric)과 이더리움(Ethereum)의 경우, 전자지갑 생성 시 소유자의 신원을 확인하지 않으며, 가상자산 송금 관련 거래 기록을 저장할 때 송금인과 수취인의 신원 정보를 포함하지 않는다. 전자지갑 소유자의 익명성은 가상자산이 자금세탁 및 테러 자금 조달에 악용되는 문제를 증가시킬 수 있다. 금융 분야에서도 이러한 익명성은 잠재적인 보안 위협으로 식별된다.



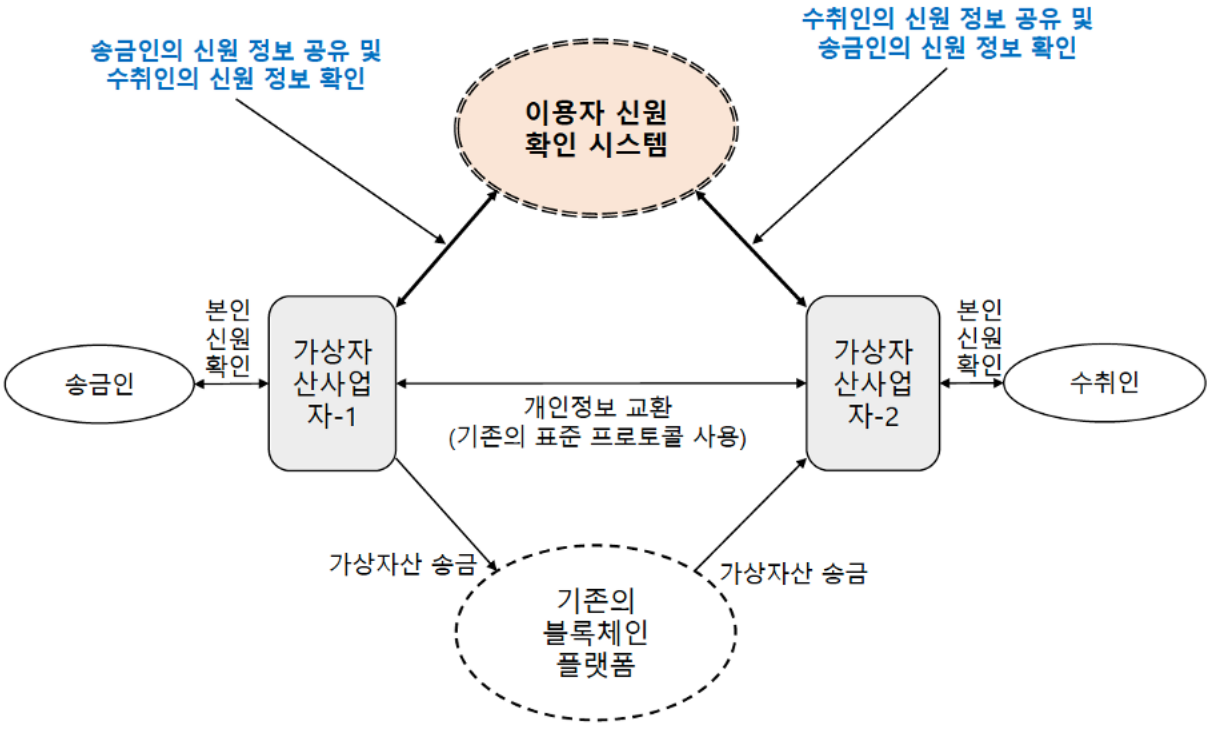
(그림 6-1) 가상자산 송금 관련 익명성

(그림 6-1)에서 기존 블록체인 및 DLT 플랫폼 환경하에서 송금인이 가상자산을 수취인에게 송금하는 경우 가상자산사업자-1은 송금인의 신원을 확인할 수 있고 가상자산사업자-3은 수취인의 신원을 확인할 수 있다. 그러나 가상자산사업자-1은 가상자산사업자-3으로부터 수취인의 신원 정보를 확인하는 것이 어려우며, 마찬가지로

가상자산사업자-3도 가상자산사업자-1로부터 송금인의 신원 정보를 확인하는 것도 어렵다. 특히 가상자산사업자 간에 이용자(송금인 및 수취인)의 신원 정보를 공유할 수 있는 인프라가 없기 때문에 국경간 가상자산 송금 시 이용자의 신원을 확인하는 것은 사실상 불가능하다.

6.2 이용자 신원 확인 방안

본 절에서는 가상자산을 송금하기 전에 VASP가 송금인과 수취인의 신원을 확인하고 공유할 수 있는 서비스 모델을 제안한다. (그림 6-2)에서 가상자산사업자-1은 송금인의 신원을 확인한다. 그리고 이용자 신원 확인 시스템을 통하여 송금인의 신원 정보를 다른 VASP와 안전하게 공유하고 수취인의 신원 정보를 확인할 수 있다. 가상자산사업자-2는 수취인의 신원을 확인한다. 그리고 이용자 신원 확인 시스템을 통하여 수취인의 신원 정보를 다른 VASP와 안전하게 공유하고 송금인의 신원 정보를 확인할 수 있다. 이용자 신원 확인 시스템은 DLT를 사용하여 VASP를 연결하고 가상자산을 송금하는 기존의 블록체인 플랫폼(예: 이더리움 등)과 완전히 독립적으로 운영된다. 가상자산사업자-1은 기존의 표준 프로토콜(예: SAML, OpenID Connect, TLS 등)을 사용하여 송금인의 개인정보를 가상자산사업자-2에게 전송한다. 그 역도 마찬가지이다.

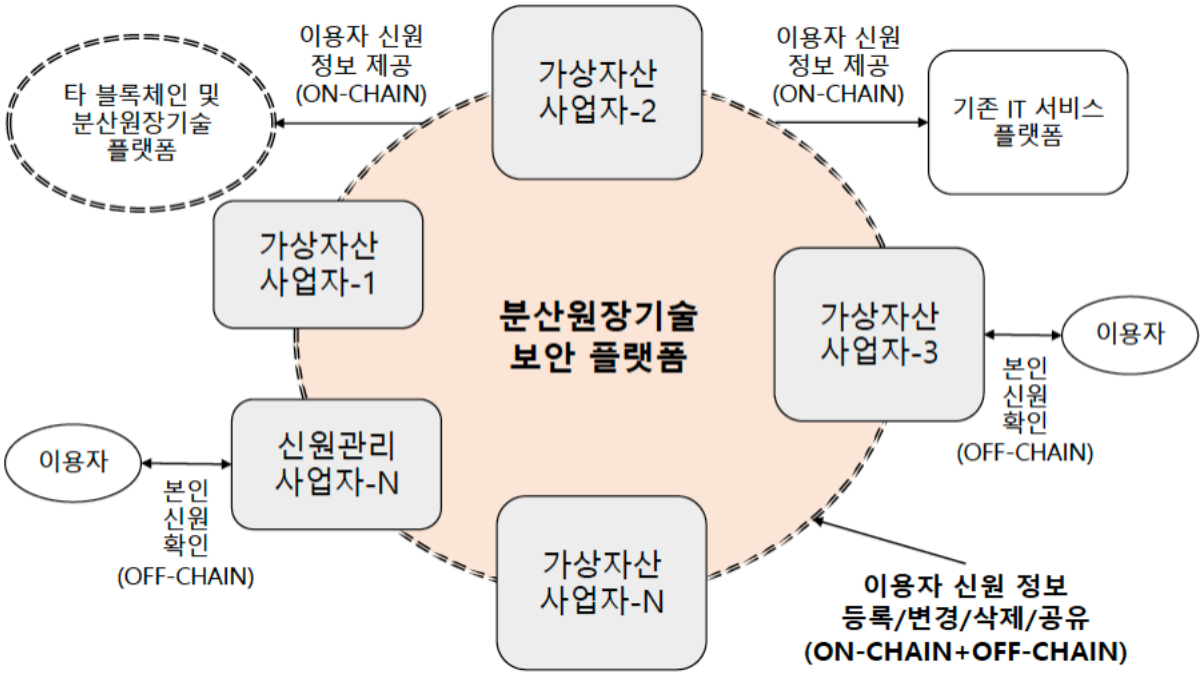


(그림 6-2) 이용자 신원 확인 서비스 모델

6.3 서비스 모델

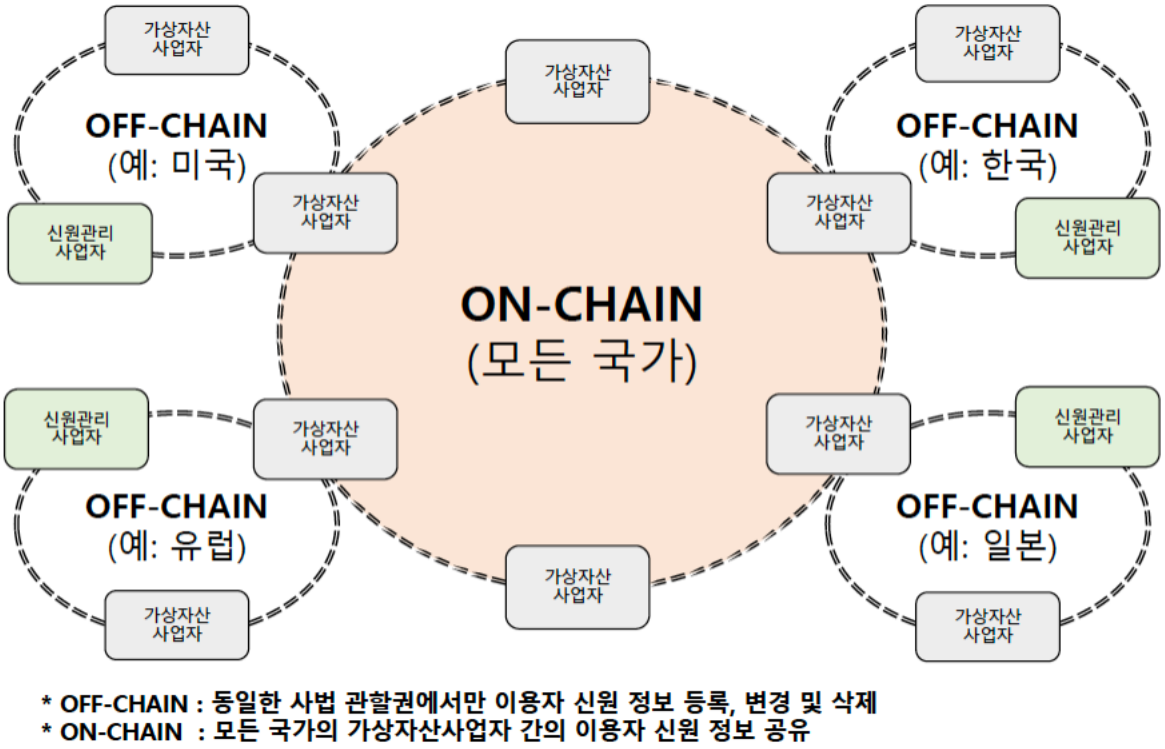
DLT 기반의 이용자 신원 확인 서비스 모델은 이용자(송금인 및 수취인), 가상자산사업자(VASP), 신원관리사업자(IDSP), 분산원장기술(DLT) 보안 플랫폼, 기존의 블록체인 및 DLT 플랫폼, 기존의 IT 서비스 플랫폼으로 구성된다. DLT 보안 플랫폼은 보안기능 요구사항을 충족하고 이용자의 신원 정보에 포함된 개인정보를 가명처리한다. 제안 서비스 모델은 VASP와 IDSP가 참여하는 DLT 시스템을 사용하여 VASP 간에 이용자의 최소한의 신원 정보를 안전하게 공유하고 검증할 수 있는 프레임워크를 제공한다. IDSP는 DID(Decentralized Identifier, 탈중앙화 식별자)를 사용하여 이용자를 식별할 수 있다.

(그림 6-3)에서는 DLT 보안 플랫폼을 기반 이용자 신원 확인 서비스 모델의 주요 구성요소와 역할을 설명한다. VASP와 IDSP는 DLT 보안 플랫폼의 노드로 참여하며, 보안기능 요구사항을 충족하는 DLT 플랫폼은 본 절의 뒷부분에서 설명한다. DLT 보안 플랫폼은 이용자 신원 정보를 등록, 변경, 삭제 및 공유할 수 있는 온체인 및 오프체인((그림 6-4) 참조)으로 구성된다. VASP, 기존 블록체인 및 DLT 플랫폼, 기존 IT 서비스 플랫폼은 온체인(ON-CHAIN)에서 이용자 신원 정보를 제공받을 수 있다. 이용자는 VASP 또는 IDSP를 통하여 오프체인(OFF-CHAIN)에 자신의 신원 정보를 제공할 수 있다.



(그림 6-3) DLT 보안 플랫폼 기반 이용자 신원 확인 서비스 모델

(그림 6-4)에서 ON-CHAIN 및 OFF-CHAIN의 노드로서 참여자를 설명하고, 또한 ON-CHAIN과 OFF-CHAIN의 서로 다른 역할을 설명한다. ON-CHAIN은 DLT 시스템 내부에서 일방향 암호화로 비식별화된 개인정보를 포함하는 이용자의 신원 정보를 처리하기 위한 일종의 저장소이다. OFF-CHAIN은 DLT 시스템 외부에서 양방향 암호화에 의해 비식별화된 개인정보를 포함한 이용자 신원 정보를 처리하는 일종의 저장소이지만 ON-CHAIN과 매우 밀접한 관련((그림 6-5) 참조)이 있다.



(그림 6-4) 온체인과 오프체인으로 구성된 DLT 보안 플랫폼

(그림 6-4)에서 보는 바와 같이, IDSP는 OFF-CHAIN의 참여자이고 VASP는 ON-CHAIN의 참여자이지만, IDSP 역할을 하는 VASP는 OFF-CHAIN의 참여자일 수 있다. OFF-CHAIN을 사용하여 동일한 관할 구역에서만 비식별화된 이용자 개인정보를 포함한 신원 정보를 등록, 변경 및 삭제할 수 있다. ON-CHAIN을 사용하여 비식별화된 이용자 개인정보를 포함한 신원 정보를 모든 국가의 VASP 간에 공유할 수 있다. ON-CHAIN은 PBFT(Practical Byzantine Fault Tolerance)와 같은 합의 알고리즘을 사용하는 허가형 비공개 분산원장시스템(Permissioned and Private DLT system)으로 구현되어야 한다.

많은 국가의 VASP는 국경간 가상자산을 송금하기 전에 개인정보를 포함한 방대한 이용자 신원 정보를 상호 공유함에 있어 이용자의 신원 정보가 변조되는 것을 방지하는 것이 매우 중요하다. 제안 서비스 모델은 중앙 집중식 데이터베이스가 아닌 DLT를 사용하여 이용자 신원 정보의 무결성을 유지하고, 자금세탁방지 관련 법규정에서 요구하는 VASP 간, VASP와 기존의 블록체인 및 DLT 서비스 제공자 간, VASP와 기존의 IT 서비스 제공자 간의 이용자 신원 확인 서비스에 활용할 수 있다.

DLT 보안 플랫폼은 다음과 같이 “TTAK.KO-12.0368, 분산원장시스템을 위한 보안기능 요구사항”에서 제공하고 있는 보안기능 요구사항을 충족해야 한다.

8 분산원장시스템의 보안기능 요구사항

8.1 식별 및 인증

분산원장시스템은 본인 확인 절차에 따라 이용자 또는 애플리케이션을 식별하고 인증하는 수단을 제공하여야 한다. 또한 거래의 중요도에 따라 강화된 인증 수단 (예: 일회용 패스워드, 공개키 인증서 등)을 적용한다. 본 보안 기능 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FIA_AFL.1 인증 실패 처리
- FIA_ATD.1 사용자 속성 정의
- FIA_SOS.1 비밀정보의 검증
- FIA_SOS.2 비밀정보의 생성
- FIA_UAU.2 모든 행동 이전에 사용자 인증
- FIA_UAU.5 다중 인증 메커니즘
- FIA_UAU.6 재인증
- FIA_UAU.7 인증 피드백 보호
- FIA_UID.2 모든 행동 이전에 사용자 식별
- FTA_MCS.1 기본적인 동시 세션 수의 제한
- FTA_SSL.3 TSF에 의한 세션 종료
- FTA_SSL.4 사용자에 의한 세션 종료

※ 6절의 6.6 식별 및 인증 클래스, 6.10 평가대상 접근 클래스를 참조한다.

8.2 보안 감사

분산원장시스템은 이용자의 행위 이력을 기록하고 안전하게 보관하여 보안 사고 발생에 대한 책임을 추적할 수 있는 수단을 제공하여야 한다. 본 보안 기능 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FAU_ARP.1 보안 경보
- FAU_GEN.1 감사 데이터 생성
- FAU_GEN.2 사용자 신원 연관
- FAU_SAR.1 감사 검토
- FAU_SAR.2 감사 검토 권한 제한
- FAU_SAR.3 선택 가능한 감사 검토
- FAU_SEL.1 선택적인 감사
- FAU_STG.1 감사 증적 저장소 보호
- FAU_STG.2 감사 데이터의 가용성 보장
- FAU_STG.3 감사 데이터 손실 예측 시 대응 행동
- FAU_STG.4 감사 데이터의 손실 방지
- FPT_STM.1 신뢰할 수 있는 타임스탬프

※ 6절의 6.2 보안감사 클래스, 6.8 평가대상의 보안기능성 보호 클래스를 참조한다.

8.3 통신 보호

분산원장시스템은 분산 원장 네트워크에 참여하는 노드 간의 중요 정보 전송 시 안전한 통신 수단을 제공하여야 한다. 또한 분산원장시스템과 외부 시스템 간의 중요 정보 전송 시 안전한 통신 수단을 제공하여야 한다. 본 보안 기능 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FCO_NRO.2 강제적인 발신 증명
- FCO_NRR.2 강제적인 수신 증명
- FPT_ITC.1 외부전송 TSF 데이터의 비밀성
- FPT_ITI.1 외부전송 TSF 데이터의 변경 탐지
- FTP_ITC.1 TSF 간 안전한 채널

※ 6절의 6.3 통신 클래스, 6.8 평가대상의 보안기능성 보호 클래스, 6.11 안전한 경로/채널 클래스를 참조한다.

8.4 암호 통제

분산원장시스템은 이용자 간의 거래 시 전자서명, 중요 정보 전송 또는 저장 시 데이터 암호화 등을 위한 암호키를 안전하게 처리(생성, 이용, 보관, 파기 등)할 수 있는 수단을 제공하여야 한다. 본 보안 기능 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FCS_CKM.1 암호키 생성
- FCS_CKM.2 암호키 분배
- FCS_CKM.3 암호키 접근
- FCS_CKM.4 암호키 파기
- FCS_COP.1 암호 연산

※ 6절의 6.4 암호 지원 클래스를 참조한다.

※ 국가·공공기관이 분산원장시스템을 운영하는 경우, 「전자정부법」에 따라 국가정보원장이 승인한 암호 모듈(검증필 암호 모듈)을 사용하여야 한다.

8.5 접근 통제

분산원장시스템은 비인가자가 중요 정보자산 (예: 분산 원장, 스마트 계약, 분산 원장 네트워크 등)에 무단으로 접근하는 것을 통제할 수 있는 수단을 제공하여야 한다. 본 보안 기능 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FDP_ACC.1 부분적인 접근통제
- FDP_ACF.1 보안속성에 기반한 접근통제

※ 6절의 6.5 사용자 데이터 보호 클래스를 참조한다.

8.6 개인정보 보호

분산원장시스템은 이용자의 개인정보가 유출 및 노출되지 않도록 안전하게 처리 (예: 수집, 이용, 보관, 파기 등)할 수 있는 수단을 제공하여야 한다. 본 보안 기능 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FDP_RIP.2 전체적인 잔여정보 보호
- FPR_PSE.2 추적가능한 가명성

※ 6절의 6.5 사용자 데이터 보호 클래스, 6.7 프라이버시 클래스를 참조한다.
※ 개인정보를 분산 원장에 저장하는 경우, 분산원장기술의 특성 상 분산 원장에 한 번 저장된 정보는 변경 또는 삭제가 어렵기 때문에 별도의 개인정보 분리 및 완전 삭제 기능을 구현하여야 한다. (예: 개인정보 암호화 후 해당 암호키 영구 삭제, 오프체인 등)
※ 개인정보의 범위 (예: 가명정보 등)는 관련 법규정을 참고한다.

8.7 데이터 보호

분산원장시스템은 이용자의 거래 데이터, 분산 원장 데이터(개인정보 포함) 등 중요 정보가 유출 또는 위·변조 되지 않도록 안전하게 전송 또는 저장하는 수단을 제공하여야 한다. 본 보안 기능 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

- FDP_DAU.2 증거 생성자의 신원을 포함한 데이터 인증
- FDP_ETC.1 보안속성 없이 사용자 데이터 유출
- FDP_ETC.2 보안속성을 포함한 사용자 데이터 유출
- FDP_ITC.1 보안속성 없이 사용자 데이터 유입
- FDP_ITC.2 보안속성을 포함한 사용자 데이터 유입
- FDP_RIP.2 전체적인 잔여정보 보호
- FDP_SDI.1 저장된 데이터의 무결성 검사
- FDP_SDI.2 저장된 데이터의 무결성 검사 및 대응 행동
- FDP_UCT.1 기본적인 전송 데이터 비밀성
- FDP_UIT.1 전송 데이터 무결성

※ 6절의 6.5 사용자 데이터 보호 클래스를 참조한다.

8.8 자원 가용성

분산원장시스템은 분산 원장 네트워크에 참여하는 노드의 시스템 자원(예: CPU, 메모리, 네트워크, 스토리지 등) 부족, 분산원장시스템을 운영하는 소프트웨어 오류 등에 대응하여 시스템 가용성을 극대화 할 수 있는 수단을 제공하여야 한다. 본 보안 기능 구현 시 다음과 같은 공통평가기준 보안기능 컴포넌트를 활용한다.

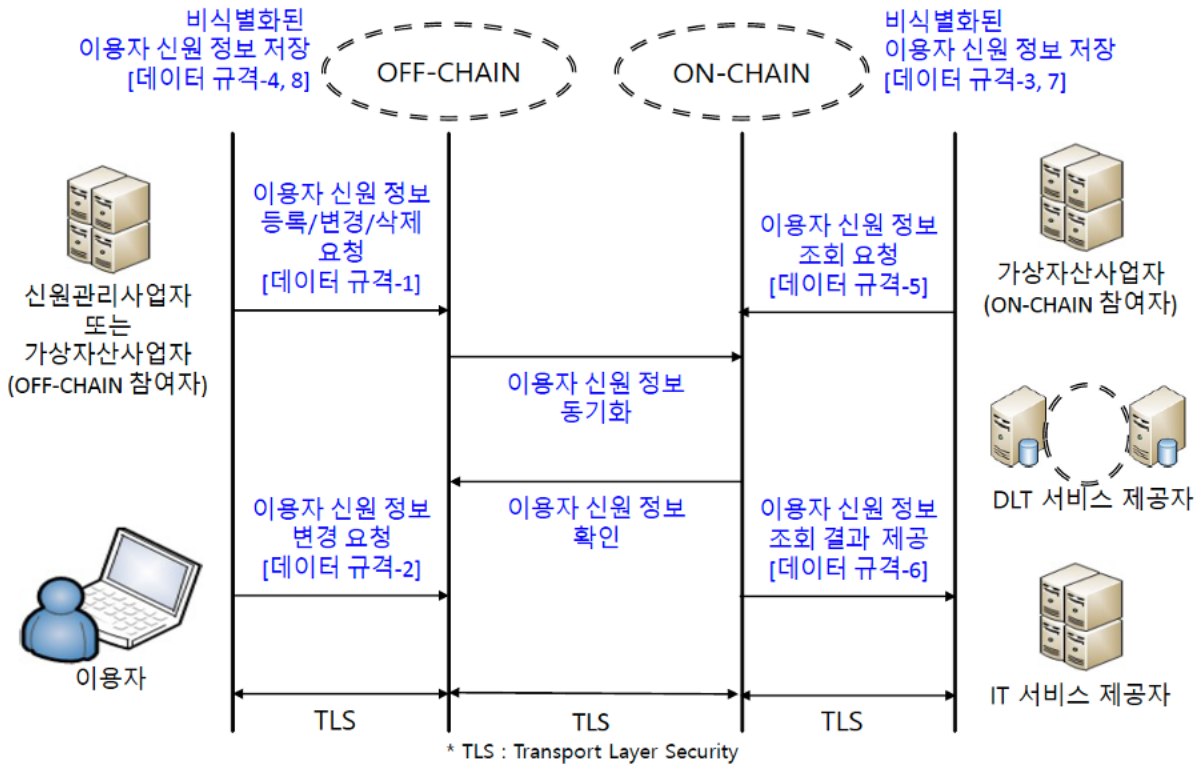
- FRU_FLT.1 오류에 대한 내성 : 부분적용
- FRU_PRS.1 자원사용 우선순위 : 부분적용
- FRU_RSA.1 최대 할당치

※ 6절의 6.9 자원 활용 클래스를 참조한다.

6.4 서비스 시나리오 및 데이터 흐름

(그림 6-5)는 VASP 또는 IDSP와 OFF-CHAIN 간의 관계, 이용자와 OFF-CHAIN 간의 관계를 설명한다. 또한 VASP와 ON-CHAIN 간의 관계, DLT 서비스 제공자 또는 IT 서비스 제공자와 ON-CHAIN 간의 관계, ON-CHAIN과 OFF-CHAIN 간의 관계에 대해

설명한다.



(그림 6-5) 서비스 시나리오 및 데이터 흐름도

DLT 기반의 이용자 신원 확인 서비스 모델에서 사용하는 데이터 규격은 데이터 규격-1~데이터 규격-8이며, 개인정보보호 관련 법규 준수를 위해 이용자의 최소한의 개인정보를 포함한다. <표 6-1>의 이용자 신원 정보에 대한 기본 데이터 규격은 10개 항목으로 구성되어 있다. 특히, 이용자 신원 정보에 포함되어 있는 개인정보를 비식별화하기 위하여 「가명정보 처리 가이드라인」에 근거하여 개인정보로 간주되는 D-1~D-4는 ON-CHAIN에서 일방향 암호화(예: SHA-256 등), OFF-CHAIN에서 양방향 암호화(예: SEED, AES-128 등)가 적용된다.

<표 6-1> 이용자 신원 정보에 대한 기본 데이터 규격

항목	암호화	값	설명
D-0	-	이용자 번호	- 이용자에게 부여한 유일한 번호 - D-1~D-3에 대한 해시값
D-1	암호화	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	암호화	이름	- 이용자(개인/법인)의 이름
D-3	암호화	인증서	- 이용자의 인증서 (예: X.509 규격)
D-4	암호화	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	-	가상자산사업자	- 이용자의 전자지갑을 관리하는 가상자산사업자의 식별자

항목	암호화	값	설명
D-6	-	신원관리사업자	- 이용자의 신원을 인증한 사업자의 식별자 - 가상자산사업자와 동일할 수 있음
D-7	-	유효성	- 이용자 신원의 유효성 - 예: Valid (거래 가능), Invalid (거래 중지), N/A (확인 불가)
D-8	-	RESERVED	RESERVED
D-9	-	RESERVED	RESERVED

<표 6-1>에서 D-0은 D-1부터 D-3까지의 해시값이자 고유번호인 이용자 번호이다. 개인정보로 간주되는 D-1은 이용자의 국적을 나타내는 국가코드로 ON-CHAIN/OFF-CHAIN에서 일방향/양방향 암호화가 적용된다. 개인정보로 간주되는 D-2는 이용자(개인 또는 법인)의 이름으로서 ON-CHAIN/OFF-CHAIN에서 일방향/양방향 암호화가 적용된다. 개인정보로 간주되는 D-3은 국제 표준 ITU-T X.509 규격을 따르는 이용자의 디지털 인증서로서 OFF-CHAIN에서 양방향 암호화가 적용된다. 개인정보로 간주되는 D-4는 이용자의 가상자산을 거래하기 위한 전자지갑으로서 ON-CHAIN/OFF-CHAIN에서 일방향/양방향 암호화가 적용된다. D-5는 이용자의 가상자산 전자지갑을 관리하는 VASP의 식별자이다. D-6은 이용자의 신원을 인증한 IDSP의 식별자로서 VASP(D-5)와 IDSP(D-6)가 동일할 수 있다. D-7은 이용자 신원의 유효성을 나타낸다. 유효성 값으로 "Valid"는 "거래 가능", "Invalid"는 "거래 불가", "N/A"는 "검증 불가"를 의미한다. VASP는 송금인의 유효성과 수취인의 유효성이 모두 "Valid", 즉 "거래 가능"을 의미하는 경우에만 가상자산을 송금해야 한다. D-8 및 D-9는 향후 사용을 위해 예약되어 있다.

(그림 6-5)에서 IDSP와 VASP는 OFF-CHAIN의 참여자로 데이터 규격-1(<표 6-2> 참조)을 사용하여 이용자의 신원 정보를 등록, 변경 및 삭제한다. <표 6-2>의 데이터 규격-1은 <표 6-1>의 기본 데이터 규격에서 파생된다.

<표 6-2> 데이터 규격-1

항목	구분	값	설명
D-0	-	RESERVED	RESERVED
D-1	필수	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	필수	이름	- 이용자(개인/법인)의 이름
D-3	필수	인증서	- 이용자의 인증서 (예: X.509 규격)
D-4	필수	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	필수	가상자산사업자	- 이용자의 전자지갑을 관리하는 가상자산사업자의 식별자
D-6	필수	신원관리사업자	- 이용자의 신원을 인증한 사업자의 식별자 - 가상자산사업자와 동일할 수 있음
D-7	필수	유효성	- 이용자 신원의 유효성 - 예: Valid (거래 가능), Invalid (거래 중지), N/A (확인 불가)

(그림 6-5)에서 이용자는 데이터 규격-2(<표 6-3> 참조)를 사용하여 OFF-CHAIN에서 자신의 신원 정보를 변경할 수 있다. <표 6-3>의 데이터 규격-2는 <표 6-1>의 기본 데이터 규격에서 파생된다.

<표 6-3> 데이터 규격-2

항목	구분	값	설명
D-0	-	RESERVED	RESERVED
D-1	필수	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	필수	이름	- 이용자(개인/법인)의 이름
D-3	필수	인증서	- 이용자의 인증서 (예: X.509 규격)
D-4	필수	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	-	RESERVED	RESERVED
D-6	-	RESERVED	RESERVED
D-7	-	RESERVED	RESERVED

(※ 이용자는 오직 자신의 전자지갑 주소만 변경할 수 있음)

(그림 6-5)에서 ON-CHAIN은 비식별화된 이용자의 개인정보를 포함한 신원 정보를 데이터 규격-3(<표 6-4> 참조)으로 저장한다. <표 6-4>의 데이터 규격-3은 <표 6-1>의 기본 데이터 규격에서 파생된다.

<표 6-4> 데이터 규격-3

항목	암호화	값	설명
D-0	-	이용자 번호	- 이용자에게 부여한 유일한 번호 - D-1~D-3에 대한 해시값
D-1	일방향	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	일방향	이름	- 이용자(개인/법인)의 이름
D-3	-	RESERVED	RESERVED
D-4	일방향	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	-	가상자산사업자	- 이용자의 전자지갑을 관리하는 가상자산사업자의 식별자
D-6	-	신원관리사업자	- 이용자의 신원을 인증한 사업자의 식별자 - 가상자산사업자와 동일할 수 있음
D-7	-	유효성	- 이용자 신원의 유효성 - 예: Valid (거래 가능), Invalid (거래 중지), N/A (확인 불가)

(그림 6-5)에서 OFF-CHAIN은 비식별화된 이용자의 개인정보를 포함한 신원 정보를 데이터 규격-4(<표 6-5> 참조)로 저장한다. OFF-CHAIN은 이용자의 신원 정보를 ON-CHAIN과 동기화를 수행한다. ON-CHAIN에서 이용자 신원 정보를 확인할 수 없는 경우 OFF-CHAIN에서 이를 확인한다. <표 6-5>의 데이터 규격-4는 <표 6-1>의 기본 데이터 규격에서 파생된다.

<표 6-5> 데이터 규격-4

항목	암호화	값	설명
D-0	-	이용자 번호	- 이용자에게 부여한 유일한 번호 - D-1~D-3에 대한 해시값
D-1	양방향	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	양방향	이름	- 이용자(개인/법인)의 이름
D-3	양방향	인증서	- 이용자의 인증서 (예: X.509 규격)
D-4	양방향	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	-	가상자산사업자	- 이용자의 전자지갑을 관리하는 가상자산사업자의 식별자
D-6	-	신원관리사업자	- 이용자의 신원을 인증한 사업자의 식별자 - 가상자산사업자와 동일할 수 있음
D-7	-	유효성	- 이용자 신원의 유효성 - 예: Valid (거래 가능), Invalid (거래 중지), N/A (확인 불가)

(그림 6-5)에서 DLT 서비스 제공자와 IT 서비스 제공자는 데이터 규격-5(<표 6-6> 참조)를 사용하여 ON-CHAIN에 이용자 신원 정보를 요청하고 데이터 규격-6(<표 6-7 참조)을 사용하여 이용자 신원 정보를 제공받는다. <표 6-6>의 데이터 규격-5 및 <표 6-7>의 데이터 규격-6은 <표 6-1>의 기본 데이터 규격에서 파생된다.

<표 6-6> 데이터 규격-5

항목	구분	값	설명
D-0	옵션	이용자 번호	- 이용자에게 부여한 유일한 번호 - D-1~D-3에 대한 해시값
D-1	필수	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	필수	이름	- 이용자(개인/법인)의 이름
D-3	-	RESERVED	RESERVED
D-4	필수	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	옵션	가상자산사업자	- 이용자의 전자지갑을 관리하는 가상자산사업자의 식별자
D-6	-	RESERVED	RESERVED
D-7	-	RESERVED	RESERVED

<표 6-7> 데이터 규격-6

항목	구분	값	설명
D-0	옵션	이용자 번호	- 이용자에게 부여한 유일한 번호 - D-1~D-3에 대한 해시값
D-1	필수	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	필수	이름	- 이용자(개인/법인)의 이름
D-3	-	RESERVED	RESERVED
D-4	필수	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	옵션	가상자산사업자	- 이용자의 전자지갑을 관리하는 가상자산사업자의 식별자
D-6	-	RESERVED	RESERVED

항목	구분	값	설명
D-7	필수	유효성	- 이용자 신원의 유효성 - 예: Valid (거래 가능), Invalid (거래 중지), N/A (확인 불가)

(그림 6-5)에서 VASP는 ON-CHAIN으로부터 데이터 규격-6(<표 6-7> 참조)을 사용하여 이용자 신원 정보를 제공받고 송금인의 유효성과 수취인의 유효성(D-7)이 모두 "Valid", 즉 "거래 가능"인지 확인한 후에 가상자산을 송금해야 한다.

(그림 6-5)에서 ON-CHAIN은 비식별화된 이용자의 개인정보를 포함한 신원 정보가 삭제되었음을 표현하기 위하여 유효성(D-7)을 "N/A", 즉 "확인 불가"로 설정하여 데이터 규격-7(<표 6-8> 참조)로 저장한다. <표 6-8>의 데이터 규격-7은 <표 6-1>의 기본 데이터 규격에서 파생된다.

<표 6-8> 데이터 규격-7

항목	암호화	값	설명
D-0	-	이용자 번호	- 이용자에게 부여한 유일한 번호 - D-1~D-3에 대한 해시값
D-1	일방향	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	일방향	이름	- 이용자(개인/법인)의 이름
D-3	-	RESERVED	RESERVED
D-4	일방향	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	-	가상자산사업자	- 이용자의 전자지갑을 관리하는 가상자산사업자의 식별자
D-6	-	신원관리사업자	- 이용자의 신원을 인증한 사업자의 식별자 - 가상자산사업자와 동일할 수 있음
D-7	-	유효성	- 이용자 신원의 유효성 - N/A (확인 불가)로 설정함

(그림 6-5)에서 OFF-CHAIN은 비식별화된 이용자의 개인정보를 포함한 신원 정보를 삭제하기 위하여 유효성(D-7)을 "N/A", 즉 "확인 불가"로 설정하여 데이터 규격-8(<표 6-9> 참조)로 저장하고, 개인정보로 간주되는 D-1~D-4를 암호화한 암호키를 영구적으로 파기한다.

<표 6-9> 데이터 규격-8

항목	암호화	값	설명
D-0	-	이용자 번호	- 이용자에게 부여한 유일한 번호 - D-1~D-3에 대한 해시값
D-1	양방향	국가 코드	- 이용자의 국적 - 예: KR(한국), US(미국) 등
D-2	양방향	이름	- 이용자(개인/법인)의 이름
D-3	양방향	인증서	- 이용자의 인증서 (예: X.509 규격)
D-4	양방향	전자지갑 주소	- 가상자산을 거래하기 위한 전자지갑 주소
D-5	-	가상자산사업자	- 이용자의 전자지갑을 관리하는 가상자산사업자의 식별자

항목	암호화	값	설명
D-6	-	신원관리사업자	- 이용자의 신원을 인증한 사업자의 식별자 - 가상자산사업자와 동일할 수 있음
D-7	-	유효성	- 이용자 신원의 유효성 - N/A (확인 불가)로 설정함

(※ 개인정보로 간주되는 D-1~D-4를 암호화한 암호키를 영구적으로 파기함)

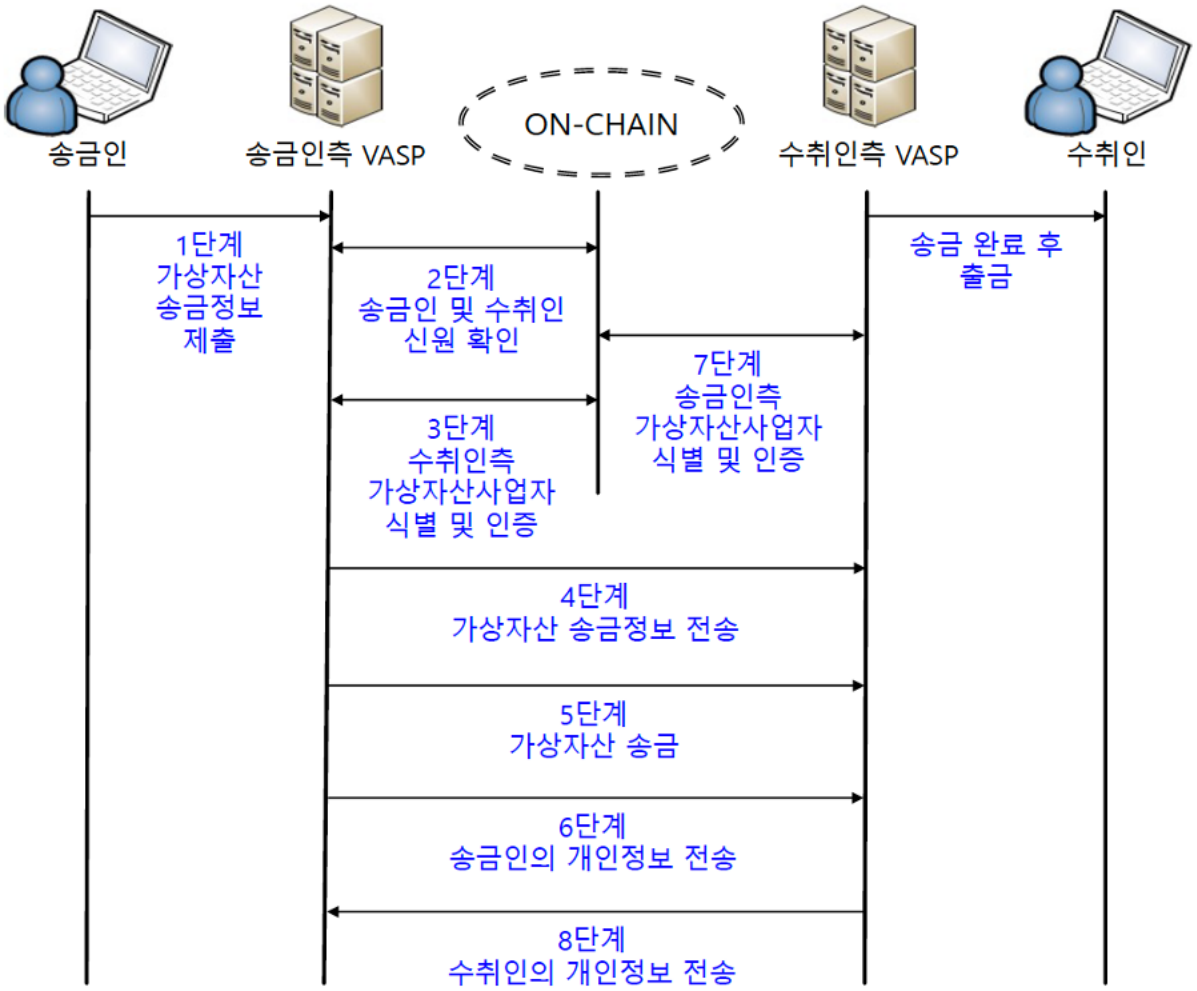
OFF-CHAIN에 저장된 D-1~D-4와 같은 개인정보를 삭제하는 방법은 D-1~D-4를 암호화한 암호키를 영구적으로 파기하는 것이다. 또한 ON-CHAIN에 저장된 D-1, D-2, D-4와 같은 개인정보는 일방향 암호화(예: SHA-256 등)가 적용되어 있기 때문에 이를 재식별하는 것은 매우 어렵다.

VASP가 일정 금액(예: 1,000미국달러)을 초과하는 가상자산을 송금하려고 할 때(5.1절 참조), 수취인측 VASP는 표준 프로토콜(예: SAML, OpenID Connect, TLS 등)을 사용하여 송금인의 개인정보(예: 주소, 주민등록번호, 생년월일 및 출생지 등)를 ON-CHAIN을 통하여 식별 및 인증된 송금인측 VASP로부터 직접 요청하고 제공받을 수 있다. 예를 들어, 1,000미국달러를 초과하는 가상자산을 송금하는 절차((그림 6-6) 참조)는 다음과 같다.

- (1단계): 송금인이 '가상자산 송금 정보(예: 송금인 이름, 송금인의 전자지갑 주소, 수취인 이름, 수취인의 전자지갑 주소, 가상자산 금액)'를 송금인측 VASP에게 제출한다.
- (2단계): 송금인측 VASP는 ON-CHAIN을 통하여 데이터 규격-6(<표 6-7> 참조)의 이용자 신원 정보와 '가상자산 송금 정보'를 비교함으로서 송금인 및 수취인의 신원 정보(유효성 포함)를 확인한다.
- (3단계): 송금인측 VASP는 ON-CHAIN을 통하여 데이터 규격-6(<표 6-7> 참조)의 이용자 신원 정보와 '가상자산 송금 정보'를 비교하여 수취인측 VASP를 식별 및 인증한다.
- (4단계): 3단계가 성공하면 송금인측 VASP는 표준 프로토콜(예: SAML, OpenID Connect, TLS 등)을 사용하여 송금인이 제출한 '가상자산 송금 정보'를 수취인측 VASP에게 직접 전송한다.
- (5단계): 2단계, 3단계, 4단계가 성공하면 송금인측 VASP가 기존의 블록체인을 사용하여 수취인측 VASP에게 가상자산을 송금한다.
- (단계 6): 5단계가 성공하면 송금인측 VASP는 자금세탁방지 법규에서 요구하는 송금인의 개인정보(예: 주소, 주민등록번호, 생년월일, 출생지 등)를 표준 프로토콜(예: SAML, OpenID Connect, TLS 등)을 사용하여 수취인측 VASP에게 직접 전송한다.
- (단계 7): 5단계가 성공하면 수취인측 VASP는 '가상자산 송금 정보'를 ON-CHAIN의 데이터 규격-6(<표 6-7> 참조)의 이용자 신원 정보와 비교하여

송금인측 VASP를 식별 및 인증한다.

- (8단계): 7단계가 성공하면 수취인측 VASP는 자금세탁방지 법규에서 요구하는 수취인의 개인정보(예: 주소, 주민등록번호, 생년월일, 출생지)를 표준 프로토콜(예: SAML, OpenID Connect, TLS 등)을 사용하여 송금인측 VASP에 직접 전송한다.



(그림 6-6) ON-CHAIN을 이용한 가상자산 송금 절차

7 보안 위협 및 보안 요구사항

7.1 보안 위협

본 절에서는 제안 서비스에 대한 보안 위협을 다음과 같이 식별하고, 일반적인 IT 서비스와 관련된 보안 위협은 다루지 않는다.

- 보안 위협-1(ST-1): 악의적인 이용자가 도용된 신원 정보를 OFF-CHAIN에 등록할 수 있다. 본 보안 위협은 자금 세탁에 악용될 수 있다.
- 보안 위협-2(ST-2): 악의적인 이용자가 OFF-CHAIN에 자신의 신원 정보를 변경할 수 있다. 본 보안 위협은 자금 세탁에 악용될 수 있다.
- 보안 위협-3(ST-3): 악의적인 IDSP(또는 IDSP 역할을 하는 VASP)가 도용된 신원 정보를 OFF-CHAIN에 등록할 수 있다. 본 보안 위협은 자금 세탁에 악용될 수 있다.
- 보안 위협-4(ST-4): 안전하지 않은 암호화 알고리즘을 사용하여 ON-CHAIN 및 OFF-CHAIN에 저장된 이용자의 개인정보를 비식별화(가명처리)할 수 있다. 본 보안 위협은 이용자의 개인정보를 재식별하기 위해 악용될 수 있다.
- 보안 위협-5(ST-5): 안전하지 않은 암호화 알고리즘은 엔티티(예: VASP, IDSP, 이용자)에서 OFF-CHAIN으로 전송되는 이용자의 개인정보를 비식별화(가명처리)하는데 사용될 수 있다. 본 보안 위협은 이용자의 개인정보를 재식별하기 위해 악용될 수 있다.
- 보안 위협-6(ST-6): OFF-CHAIN에서 ON-CHAIN으로 전송되는 이용자의 개인정보를 비식별화(가명처리)하기 위해 안전하지 않은 암호화 알고리즘을 사용할 수 있다. 본 보안 위협은 이용자의 개인정보를 재식별하기 위해 악용될 수 있다.
- 보안 위협-7(ST-7): 안전하지 않은 암호화 알고리즘은 ON-CHAIN에서 엔터티(예: VASP, DLT 서비스 공급자, IT 서비스 공급자)로 전송되는 이용자의 개인정보를 비식별화(가명처리)하는 데 사용할 수 있다. 본 보안 위협은 이용자의 개인정보를 재식별하기 위해 악용될 수 있다.
- 보안 위협-8(ST-8): 악의적인 이용자는 OFF-CHAIN에서 자신의 신원 정보를 변경한 것을 부인할 수 있다. 본 보안 위협은 자금 세탁에 악용될 수 있다.
- 보안 위협-9(ST-9): 악의적인 IDSP(또는 IDSP 역할을 하는 VASP)가 이용자의 신원 정보를 OFF-CHAIN에 등록한 것을 부인할 수 있다. 본 보안 위협은 자금 세탁에 악용될 수 있다.

7.2 보안 요구사항

7.1절에서 식별된 보안 위협을 완화시킬 수 있는 보안 요구사항은 다음과 같다.

- 보안 요구사항-1(SR-1): 제안 서비스는 IDSP(또는 IDSP 역할을 하는 VASP)가

이용자의 신원 정보를 OFF-CHAIN에 직접 등록하고, 이용자가 자신의 신원 정보를 OFF-CHAIN에 등록하지 못하도록 해야한다.

- 보안 요구사항-2(SR-2): 제안 서비스는 이용자가 OFF-CHAIN에서 최소한으로 자신의 신원 정보를 변경할 수 있도록 하고, VASP가 OFF-CHAIN에서 변경된 신원 정보를 검증하도록 해야한다.
- 보안 요구사항-3(SR-3): 제안 서비스는 VASP가 OFF-CHAIN에 참여하기 전에 VASP가 정부 당국에서 발급한 공식 라이선스를 보유하고 있는지 확인해야 한다. (「특정 금융거래정보의 보고 및 이용 등에 관한 법률」제2조(신고) 참조)
- 보안 요구사항-4(SR-4): 제안 서비스는 ON-CHAIN 및 OFF-CHAIN에 저장된 이용자의 개인정보를 비식별화(가명처리)하기 위하여 안전한 암호화 알고리즘(예: SHA-256 및 AES-128)을 제공해야 한다.
- 보안 요구사항-5(SR-5): 제안 서비스는 전송구간에서 이용자의 개인정보를 비식별화(가명처리)하기 위하여 안전한 암호 알고리즘 및 프로토콜(예: TLS)을 제공해야 한다.
- 보안 요구사항-6(SR-6): 제안 서비스는 이용자가 OFF-CHAIN에서 자신의 신원 정보를 변경할 때 해당 이용자의 PKI 기반 전자서명을 검증해야 한다.
- 보안 요구사항-7(SR-7): 제안 서비스는 IDSP(또는 IDSP 역할을 하는 VASP)가 OFF-CHAIN에 이용자의 신원 정보를 등록할 때 IDSP(또는 IDSP 역할을 하는 VASP)의 PKI 기반 전자서명을 검증해야 한다.

<표 7-1> 보안 위협과 보안 요구사항 간의 관계

	SR-1	SR-2	SR-3	SR-4	SR-5	SR-6	SR-7
ST-1	O						
ST-2		O					
ST-3			O				
ST-4				O			
ST-5					O		
ST-6					O		
ST-7					O		
ST-8						O	
ST-9							O

(※ ST=보안 위협, SR=보안 요구사항)

<표 7-1>에서 보는 바와 같이, SR-1은 ST-1을 방지할 수 있고 SR-2는 ST-2를 방지할 수 있다. SR-3은 ST-3을 방지할 수 있고 SR-4는 ST-4를 방지할 수 있다. SR-5는 ST-5, ST-6, ST-7을 방지할 수 있다. SR-6은 ST-8을 방지할 수 있고 SR-7은 ST-9를 방지할 수 있다.

부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

지식재산권 확약서 정보

아래에 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

해당 사항 없음.

부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

시험인증 관련 사항

해당 사항 없음

부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

본 표준의 연계(family) 표준

해당 사항 없음

부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

참고 문헌

아래 기재된 참고 문헌의 발간일이 기재된 경우, 해당 표준(문서)의 해당 버전에 대해서만 유효하며, 연도를 표시하지 않은 경우에는 해당 표준(권고)의 최신 버전을 따른다.

금융위원회, “특정 금융거래정보의 보고 및 이용 등에 관한 법률(법률 제17299호)”, 2021년 5월.
금융정보분석원, “특정 금융거래정보 보고 및 감독규정(금융정보분석원고시 제2021-1호)”, 2021년 3월.
개인정보보호위원회, “개인정보 보호법(법률 제16930호)”, 2020년 8월.
TTAK.KO-12.0336, 블록체인 용어정의, 2018년 12월.
TTAK.KO-12.0368, 분산원장시스템을 위한 보안기능 요구사항, 2020년 12월.
ITU-T X.1400, Terms and definitions for distributed ledger technology, October 2020.
개인정보보호위원회, “가명정보 처리 가이드라인”, 2020년 9월.
Park, Keundug, and Heung-Youl Youm. 2021. "Proposal for Customer Identification Service Model Based on Distributed Ledger Technology to Transfer Virtual Assets" Big Data and Cognitive Computing 5, no. 3: 31. https://doi.org/10.3390/bdcc5030031

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	2021.12.8.	제정 TTAK.KO-12.0374	-	개인정보보호/ID관리, 블록체인 보안 (PG502)