

# Trusted Web 구축을 위한 기술 및 보안연구 (최종 보고서)

수행기관: 한국시스템보증(주)

2023. 12.

## 제 출 문

한국인터넷진흥원 원장 귀하

본 보고서를 “Trusted Web 구축을 위한 기술 및 보안연구”의  
최종 연구결과 보고서로 제출합니다.

2023 년 12 월 11 일

수탁 기관 : 한국시스템보증(주)

연구책임자 : 이 사 이강석

참여연구원 : 부 장 조경호

부 장 김남균

책 임 장상민

선 임 이재형

# 목 차

제 1 장 Trusted Web 개요 .....	1
제 1 절 현 인터넷/웹의 현안과 문제점 .....	1
제 2 절 Trusted Web 개요 .....	9
제 2 장 국가별 Trusted Web 구축 동향 .....	15
제 1 절 유럽 국가 .....	15
제 2 절 아메리카 .....	30
제 3 절 아시아 .....	33
제 3 장 Trusted Web 기반 기술 .....	44
제 1 절 블록체인(Blockchain) .....	44
제 2 절 대체 불가능 토큰(NFT) .....	52
제 3 절 분산 ID(Decentralized Identity) .....	54
제 4 절 Digital Wallet .....	64
제 5 절 Solid Project .....	70
제 4 장 Trusted Web 설계 .....	78
제 1 절 Trusted Web 아키텍처 설계 .....	78
제 2 절 Trusted Web 서비스 설계 .....	83
[참고문헌] .....	101
<첨부 1> 일본: Trusted Web Use Case 분석 .....	103
<첨부 2> 일본: Trusted Web Framework 분석 .....	131

## 〈표 차례〉

[표 1] 침해유형별 사례(총 79건) .....	5
[표 2] 주요 국가의 온라인 플랫폼 기업 규제 제도 .....	7
[표 3] 국가별 테스트된 유스케이스 .....	22
[표 4] 블록체인 프로세스 및 내용 .....	45
[표 5] 분산원장의 특징 .....	46
[표 6] 분산원장 구성요소 .....	46
[표 7] 블락(Block) 구성요소 .....	47
[표 8] 스마트 컨트랙트 구성요소 .....	48
[표 9] 스마트 컨트랙트 동작 과정 .....	50
[표 10] 분산 합의 알고리즘의 종류 .....	51
[표 11] NFT 주요 구성요소 .....	52
[표 12] NFT 동작 과정 .....	54
[표 13] DID Documents 구성요소 .....	58
[표 14] DID Authentication의 작동 방식 .....	59
[표 15] DID Resolver의 작동 방식 .....	60
[표 16] Decentralized Key Management System (DKMS)의 구성 요소 .....	63
[표 17] Decentralized Key Management System (DKMS)의 동작 과정 .....	64
[표 18] Wallet Controller의 주요 기능 .....	66
[표 19] Protocol Manager의 주요 기능 .....	67
[표 20] User Profile Manager의 주요 기능 .....	68
[표 21] Instrument Manager의 주요 기능 .....	68
[표 22] Communication Manager의 주요 기능 .....	69
[표 23] Digital Wallet의 처리 흐름 .....	69
[표 24] Trusted Web의 실현 목표 및 효과 .....	132
[표 25] Trusted Web 구현 기능 및 실현 수단 .....	133

## 〈그림 차례〉

(그림 1) 가짜뉴스와 이에 대한 사회적 논쟁 .....	1
(그림 2) 동의정도에 대한 글로벌 순위 (출처, 입소스, 단위 %)	2
(그림 3) 중고거래 사기유형과 중고거래 피해규모(출처, 유동수 의원실)	3
(그림 4) 개인정보 침해사고·상담 건수 .....	4
(그림 5) 온라인 플랫폼-입점업체간 불이익제공 관련 분쟁조정 추이 .....	6
(그림 6) eIDAS 2.0 구성요소 .....	17
(그림 7) EUDIW 생태계 .....	17
(그림 8) eIDAS 노드를 통한 회원국 간 eID 사용 예 .....	18
(그림 9) EUDI Wallet 기능 .....	19
(그림 10) EUDI Wallet의 인터페이스 .....	19
(그림 11) SSI 아키텍처에 매핑된 eIDAS Toolbox .....	20
(그림 12) EWC 참여 국가 .....	21
(그림 13) IDunion 구성요소: 사용된 기술 및 표준 .....	26
(그림 14) SSI 기술을 사용하여 자격증명을 확인하는 일반 프로세스 .....	27
(그림 15) 트러스트 프레임워크와 구성요소간의 관계 .....	28
(그림 16) PCTF 구성요소 .....	32
(그림 17) Trusted Web의 방향성과 목표 .....	33
(그림 18) 구직사이트 Trusted Web 구성도 .....	34
(그림 19) 구직사이트 Trusted Web 동작 절차 .....	35
(그림 20) NDI Stack 피라미드 .....	36
(그림 21) 뉴질랜드의 디지털 ID 시스템(안) .....	39
(그림 22) Account Aggregator Framework .....	41
(그림 23) 모바일 신분증 서비스 플랫폼 .....	42
(그림 24) 공공마이데이터 유통 체계 .....	42
(그림 25) 블락체인 프레임워크 .....	44
(그림 26) DIDs 프레임워크 .....	55
(그림 27) 분산 ID 관리 구조 및 발급/검증 절차 .....	55
(그림 28) Digital Wallet 아키텍처 .....	65
(그림 29) Digital Wallet 구성요소 .....	66

(그림 30) Solid 구성요소 .....	70
(그림 31) WebID 솔루션 .....	71
(그림 32) lod-cloud.net에 연결된 개방형 데이터 클라우드 .....	72
(그림 33) Solid 아키텍처 구성도 .....	75
(그림 34) Solid 플랫폼 예시 .....	76
(그림 35) Pod 아키텍처 .....	76
(그림 36) Trusted Web Architecture .....	79
(그림 37) 검증가능 데이터 작업의 예시 .....	80
(그림 38) 전체 경로의 검증 가능성 평가 .....	82
(그림 39) 노드, 메시지, 트랜잭션, 전송간의 관계 및 프로세스 .....	83
(그림 40) 통합 크리덴셜을 통한 다양한 서비스 접근 구성도 .....	84
(그림 41) 다양한 신뢰증명 과정 예제 .....	85
(그림 42) 데이터 신뢰성을 위한 구성도 .....	85
(그림 43) Chain of Custody 예제 .....	88
(그림 44) Trusted Web 아키텍처 모델 .....	89
(그림 45) Trusted Web 서비스 구성요소 .....	91
(그림 46) 인터넷 Platform 서비스 사업자 .....	93
(그림 47) Trusted Web의 4가지 핵심기능 .....	94
(그림 48) 통합 ID 생성 과정 .....	95
(그림 49) 신뢰통신 과정 .....	97
(그림 50) VP(Verifiable Presentation) Policy 생성 예 .....	97
(그림 51) 동적동의 과정 .....	98
(그림 52) 데이터 추적 개념도 .....	99

## [ Abbreviation ]

- o DApp: Decentralized Application
- o DID: Distributed IDentity
- o DLT: Distributed Ledger Technology
- o eIDAS: electronic IDentification, Authentic and trust Services
- o eSSIF: European Self-Sovereign Identity Framework
- o EUDIW: EU Digital Identity Wallet
- o IDEF: IDentity Ecosystem Framework
- o IDIA: Identity for All
- o NHI: National Health Insurance
- o NIST: National Institute of Standards and Technology
- o NSN: National Student Number
- o NSTIC: National Strategy for Trusted Identities in Cyberspace
- o OIDF: OpenID Foundation
- o OIX: Open Identity Exchange
- o QTSP: Qualified Trust Service Provider
- o IRD: Individual Taxpayer's Identification Number
- o SSI: Self-Sovereign Identity
- o TDIF: Trusted Digital Identity Framework
- o TSP: Trust Service Provider
- o VC: Verifiable Credential or Verify Code
- o VP: Verifiable Presentation
- o W3C: World Wide Web Consortium

# 제 1 장 Trusted Web 개요

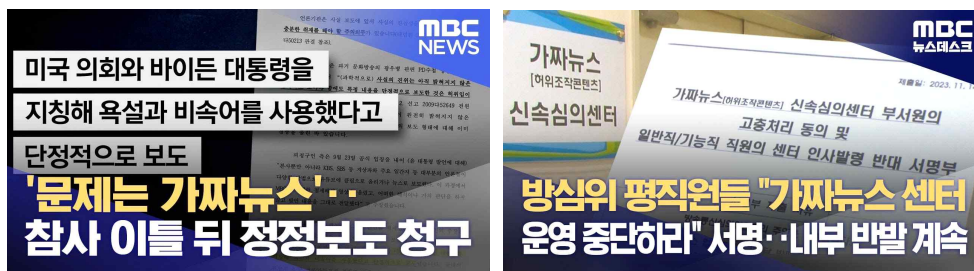
## 제 1 절 현 인터넷/웹의 현안과 문제점

인터넷은 현대 사회에서 중요한 역할을 담당하고 있지만, 여러 가지 문제점도 동시에 가지고 있다. 특히 신뢰할 수 없는 정보와 가짜뉴스로 인해 사회 혼란을 가중시키고 있으며, 데이터 위·변조, 데이터 유·노출 등 보안사고가 지속적으로 증가하고 있다. 보안취약점을 악용한 사이버 침해사고 등은 실 세계를 위협하고 있다.

### 1. 인터넷 상 데이터의 신뢰성

인터넷 상 데이터의 신뢰성은 가짜뉴스와 같은 거짓 정보로부터의 보호가 핵심적인 이슈이다. 가짜뉴스는 소셜 미디어와 온라인 플랫폼을 통해 빠르게 확산되어 사회적 혼란을 야기할 수 있다.

가짜뉴스(Fake news)는 2010년 초·중반부터 급증한 이후 2017년 미국 대통령 선거에서 엄청난 위력을 발휘하며 뜨거운 화두로 부상하였다. 이러한 배경에는 SNS 시대가 열리면서 초연결 사회인프라가 확산되어 정보를 무차별적으로 확산시킬 수 있는 인터넷 서비스가 주효했다. 실제로 가짜뉴스는 페이스북 등 SNS를 통해 주로 확산되고 있다.



(그림 1) 가짜뉴스와 이에 대한 사회적 논쟁

가짜뉴스의 영향력은 갈수록 확대되고 있으며, 이른바 ‘진실에 거짓을 섞는 양상’으로 고도화 되면서 여론을 호도하는 경우가 늘고 있다. 마케팅 여론조사 기관인 입소스(Ipsos)의 2018년 가짜뉴스의 심각성에 관한 조사에 따르면, ‘동의정도: 사람들은 사실보다 원하는 것을 믿는다’의 정도가 전 세계적으로 60% 정도로 나타났다. 다음 그



림은 전세계 가짜뉴스에 대한 동의정도를 보여준다. 한국은 전세계 23위로 약 53%의 설문 참여자가 사실보다 원하는 것을 믿는다고 조사되었다.



(그림 2)동의정도에 대한 글로벌 순위 (출처, 입소스, 단위 %)

인터넷 상의 정보범람은 불완전한 인지 능력을 가진 사람들에게 영향을 미칠 수 있다. 이러한 상황에서 거짓 정보가 추가되어 확증편향을 유발<sup>1)</sup>할 수 있으며, 결과적으로 가짜뉴스가 확산 될 가능성이 높아지게 된다.

인터넷을 통한 가짜뉴스 확산 등 문제를 해결하기 위해, 프랑스, 미국 등 여러 나라에서는 인지능력 향상을 위한 ‘미디어 리터러시(Media Literacy) 교육’을 추진해 왔다. 미디어 리터러시 교육은 정보평가를 위한 논리적 사고, 참여, 소통, 협업에 필요한 윤리적 태도와 책임감, 디지털 시대의 직업윤리 등을 모두 포함하고 있다.

2013년 프랑스에서는 미디어와 정보교육법 조항을 신설하였으며, 2016년 미국 워싱턴 주에서는 디지털 시민의식(Digital Citizenship)에 관한 법률을 제정하였다. 2018년 캘리포니아주에서는 학교 교육과정에 미디어 리터러시 교육을 정식으로 포함하였으며, 2020년에는 미국 14개 주에서 디지털 리터러시 교육을 위한 법제화를 추진하는 등 인터넷 정보에 대한 인지능력을 향상 시키기 위해 노력하고 있다.

하지만, ‘미디어 리터러시’와 같은 교육을 통해 인간의 불완전한 인지능력을 향상시키고 인터넷 상 데이터의 신뢰성을 확보하는 방법에는 한계점이 존재한다. 법·제도적인 가이드에 따라, 교육기관의 이행과 교육·학습효과가 나타나야 한다. 즉, 인간의 학습능력과 실행능력에 의존한다면, 인터넷 상 데이터의 신뢰성을 확보를 기대하기에는 역부족일 것이다.

1) 인디애나 대학의 Filippo Menczer 교수는 “가짜뉴스는 사람의 불완전한 주의집중 범위(attention span)와 확증편향(confirmatio bias) 습성 때문”이라고 주장. 출처: Filippo Menczer, “The science of fake news”, American Association for the Advancement of Science, 2018.

## 2. 데이터 주체에 대한 신뢰성

인터넷의 데이터 주체에 대한 신뢰성은 주로 개인정보 보호, 온라인 신원확인, 디지털 신뢰 등의 측면에서 중요한 요소이다. 개인정보 보호는 사용자의 민감한 정보가 안전하게 다루어지고 활용되는지를 보장해야 하며, 법적인 규정과 보안조치를 준수하는 기업 및 플랫폼은 데이터 주체에게 신뢰를 제공해야 한다.

하지만, 기업 및 플랫폼의 법적인 규정과 보안조치의 사각지대에서 여전히 데이터 주체에 대한 신뢰성이 문제가 되고 있다. 현재 인터넷 상 데이터 주체에 대한 신뢰성 문제로 온라인 거래의 사기, 인터넷 상의 평판조작, 소셜 미디어의 허위정보 등이 급증하고 있다.

플랫폼을 통한 중고거래에서, 사기꾼은 쇼핑몰이나 중고 거래 사이트에 물품을 편집하여 가짜 상품을 판매한다. 사기꾼은 판매 대금이 입금되면 연락을 끊고 잠적하고, 이후 다른 플랫폼에서 계정을 다시 생성하여 신분을 세탁한다. 이러한 사기는 상습적인 사기<sup>2)</sup>로 반복된다.



(그림 3) 중고거래 사기유형과 중고거래 피해규모(출처, 유동수 의원실)

형법 제347조에 따르면 “사람을 기망하여 재물의 교부를 받거나 재산상의 이익을 취득한 자는 10년 이하의 징역또는 2천만원 이하의 벌금에 처한다” 라고 사기에 대한 처벌방법을 정의하고 있다.

사이버 사기를 예방하기 위해 정부와 플랫폼은 사기통합 조회, 경찰청 사이버 캡,

2) 상습사기의 정의: 사기행위를 하는 습벽속성과 자본적 또는 경제활동상의 의존성으로 인한 강박성 습벽. 출처: 대법원 판결 판례 1999.11.26. 선고99도3929

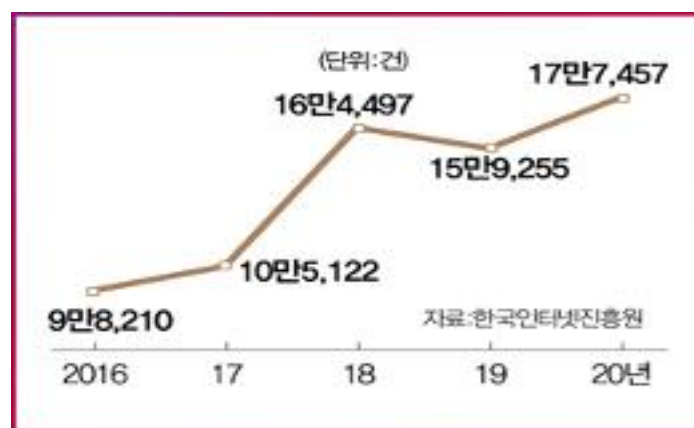
사기 피해 사례 검색 등의 사기 조회 서비스를 제공하고, 사용자의 거래 주의 당부와 추가 송금 요구시 거래 중단 등의 주의를 당부하고 있다.

사이버 사기 방지를 위해 형벌을 가중하거나 사용자에게 홍보함으로써 사용자에게 책임을 떠 넘기는 방법외에 보다 효과적인지 방법에 대한 고안이 필요하다.

### 3. 데이터 취급자에 대한 신뢰성

인터넷 상 데이터 취급자에 대한 신뢰성 문제는 주로 데이터 취급자의 데이터 수집, 보관, 처리, 공유 등과 관련된 활동에서 발생한다. 많은 기업과 서비스 플랫폼이 대규모로 사용자 데이터를 수집하고 있으며, 이에 대한 목적과 범위를 명확히 알리지 않거나 사용자 동의 없이 수집하는 경우로 인해 사생활 침해 우려가 발생하고 있다. 또한, 수집된 데이터의 부정확성과 품질문제는 실제로 수집된 데이터가 정확하고 신뢰성 있는지에 대한 의문을 불러일으킨다.

한국인터넷진흥원의 개인정보 침해사고 및 상담건수 추이를 보면, 2016년도 이후 꾸준히 증가하며, 2020년에는 약 18만건의 침해사고·상담건수를 기록했다.



(그림 4) 개인정보 침해사고·상담 건수

2023년 발간된 개인정보보호위원회의 분쟁조정 사례집에 따르면, 전체 79건중 목적 외 이용 또는 제3자 제공이 23건으로 높게 나타났으며, 개인정보 취급자의 누설·유출·훼손이 16건, 동의 없는 개인정보 수집·이용이 15건, 정보주체의 열람·정지·철회 등 요구 불응이 13건 순으로 나타났다.

[표 1] 침해유형별 사례(총 79건)

침해유형	건수
목적외 이용 또는 제3자 제공	23
개인정보 취급자의 누설·유출·훼손	16
동의 없는 개인정보 수집·이용	15
정보주체의 열람·정지·철회 등 요구 불응	13
안전성 확보조치 미비	5
보유기간 경과 또는 목적달성 후 미파기	2
기타(과도한 개인정보 수집 등)	5

※ 출처: 개인정보보호위원회, 분쟁조정 사례집(2023년)

서비스 플랫폼 사업자의 개인정보 활용 ‘목적외 이용 또는 제3자 제공’에 대해서는 2023년 개정된 개인정보보호법에 따라, 개인정보의 활용에 대해 관보 또는 인터넷 홈페이지 등에 게재하도록 변경되었다.

[ 개인정보보호법 제18조 (개인정보의 목적 외 이용·제공 제한) ]

④ 공공기관은 제2항제2호부터 제6호까지, 제8호부터 제10호까지에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 보호위원회가 고시로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.

하지만, 서비스 플랫폼 사업자의 개인정보 제공 및 활용에 대한 검증주체와 절차 부재로 인해 개인정보의 오남용 가능성이 여전히 남아 있으며, 데이터 취급자에 대한 신뢰성에 대한 검증 문제가 대두되고 있다.

#### 4. 온라인 플랫폼의 거래 공정성

온라인 플랫폼의 거래 불공정성은 판매자와 구매자 간의 균형이 깨지거나, 플랫폼 운영자의 행위로 인해 공정한 시장 경쟁이 저해되는 문제를 의미한다.

개인정보 수집과 이용은 온라인 플랫폼의 거래불공정성과 직접적으로 연결되어 있다. 많은 온라인 서비스와 플랫폼은 사용자의 개인정보를 수집하고, 수집된 데이터를 이용해 맞춤형 서비스를 제공한다.

서비스 사업자와 플랫폼의 데이터가 축적됨에 따라 서비스 수익은 증가하게 되고,

거대한 플랫폼으로 성장하게 된다. 시장에서의 정보의 독과점은 승자독식 체제를 갖추고, 플랫폼 사업자와 입점업체 또는 개인간 거래 불공정 형태가 발생하게 된다.

2023년 한국공정거래조정원에 따르면, 온라인 플랫폼과 입점업체간 불이익 제공 관련 분쟁조정 추이가 2019년 이래 지속적으로 증가하고 있으며, 2023년에는 무려 104건이 발생했다고 보고하고 있다.



(그림 5) 온라인 플랫폼-입점업체간 불이익제공 관련 분쟁조정 추이  
(출처: 한국공정거래조정원, 2023.8)

또한, 공정거래위원회는 온라인 플랫폼과 입점업체간 불공정 사례를 다음과 같이 세부적으로 제시하고 있다.

- 카카오 모빌리티: 카카오 가맹택시 ‘콜’ 몰아주기(조사중)
- 쿠팡: 자체브랜드 상품 검색결과 상위 노출
- 야놀자·여기어때: 광고노출 순서 정보 미제공
- 네이버 쇼핑: 검색 알고리즘 조작해 자사 상품·동영상 상단 노출

각 국가에서는 이러한 온라인 플랫폼 기업을 규제하기 위해 다음과 같이 제도를 개발하고 시행하고 있다.

[표 2] 주요 국가의 온라인 플랫폼 기업 규제 제도

국가	제도	비고
유럽연합 (EU)	<ul style="list-style-type: none"> <li>- 디지털 시장법</li> <li>· 플랫폼 내 자사 서비스 우대, 결합판매, 제3자 제공 서비스 접근 방해 금지 등 독점화 기도 행위 규율</li> </ul>	2024년 상반기 시행
	<ul style="list-style-type: none"> <li>- 온라인 플랫폼 공정성 및 투명성 규칙</li> <li>· 플랫폼 사업자와 입점 업체 간 거래 불공정행위를 규제</li> </ul>	2020.7월 시행
미국	<ul style="list-style-type: none"> <li>- 플랫폼 반독점 패키지 5대 법안</li> <li>· 플랫폼 기업의 자사 상품 우대, 이해상충 사업 겸업, 신생 기업인수·합병 금지 등</li> </ul>	2022년 법제사법위 통과
한국	<ul style="list-style-type: none"> <li>- 온라인 플랫폼 중개거래 공정화에 관한 법률</li> <li>· 계약기간 변경·해지 시 서면 교부, 거래해지 30일 전 이유 통지, 불공정 행위 공정위 과징금 허용 등</li> </ul>	2023.1 발의. 국회 계류중

플랫폼은 사용자들이 서로 협력하고 원만한 관계를 유지할 수 있도록 지원하며, 분쟁이 발생한 경우 중재나 조정을 통해 문제를 해결하여야 한다. 이를 통해 사용자들은 자발적으로 타협하여 상호간의 이익을 극대화할 수 있다. 하지만 모든 플랫폼이 이러한 정화 및 타협 절차를 제공하는 것은 아니기 때문에 사용자들은 플랫폼의 정책을 확인하고 이를 고려하여 플랫폼을 이용할 필요가 있다.

## [ 현 인터넷/웹의 문제점과 현안 요약 ]

### ○ 현 인터넷/웹의 개요

- 인터넷과 웹은 광범위한 정보접근 및 다양한 서비스 창출이 가능한 글로벌 공통인프라
- 디지털 사회 안전·신뢰성 보장을 위한 적절한 메커니즘 부재
  - 사용자는 플랫폼 운영자의 신뢰성에 의존적
- 현 인터넷/웹의 장점을 활용하되, 신뢰성 보장을 위한 거버넌스와 운영 메커니즘 필요

### ○ 현 인터넷/웹의 문제점

- **인터넷상 교환되는 데이터의 신뢰성 결여**: 인터넷을 통해 전송되는 데이터의 신뢰성 부족으로 데이터가 손실되거나 손상될 수 있으며, 이로 인해 정보의 정확성과 무결성에 문제가 발생
- **데이터 주체(송신자)에 대한 신뢰성 결여**: 데이터를 보내는 주체의 신뢰성이 부족하여 송신자가 잘못된 정보를 제공하거나 의도적으로 데이터를 조작할 수 있으며, 이로 인해 신뢰성 있는 데이터 교환에 어려움
- **데이터 취급자(수신자)에 대한 신뢰성 검증 부재**: 데이터를 받는 취급자의 신뢰성을 검증하는 체계가 부족하므로 데이터를 수신하는 측에서 적절한 검증 및 확인 절차를 수행하지 않으면, 잘못된 정보를 수용하거나 신뢰할 수 없는 데이터 처리
- **온라인 플랫폼의 거래 공정성 신뢰 저하**: 온라인 플랫폼에서의 거래 과정에서 공정성에 대한 신뢰 저하로 플랫폼의 중재나 분쟁해결 체계의 불명확성, 부당한 조건 및 제한, 사기나 부정행위에 대한 적절한 대응 부재 등과 같이 신뢰성 저하

### ○ 발생 가능한 문제점에 대한 사례

- **가짜뉴스 등 허위정보 유통으로 인한 사회적 분열**: 가짜뉴스와 허위정보의 유통은 사회적 분열 초래. 잘못된 정보를 믿고 퍼뜨리는 사람들 사이에 갈등이 생길 수 있으며, 신뢰성 있는 정보에 대한 신뢰도 저하 우려
- **판매 사기 및 신분세탁으로 인한 전자상거래 불신**: 전자상거래에서의 판매 사기와 신분세탁은 소비자들에게 불신 야기. 부정확한 상품 정보, 사기적인 판매 행위, 개인정보 유출 등은 전자상거래 시장의 신뢰도 저하
- **민감정보의 무분별한 수집·가공 및 악용**: 민감정보의 무분별한 수집, 가공 및 악용은 개인의 프라이버시와 보안에 위협. 개인정보의 불법적인 수집 및 악용은 사생활 침해와 신용정보 유출 등을 초래 가능성
- **정보독점 및 활용(승자독식)으로 인한 거래 불공정**: 일부 기업이 정보를 독점하고 활용하는 경우, 거래의 공정성 훼손. 이로 인해 경쟁력이 약한 기업은 불이익을 받을 수 있으며, 시장의 불균형 야기

## 제 2 절 Trusted Web 개요

Trusted Web에 관해서는 아직까지 공인된 기관을 통해 공식적으로 논의되거나 정의된 개념은 존재하지 않는다.

일본의 내각관방 디지털시장경쟁본부는 2022년 8월, Trusted Web White Paper Ver. 2.0을 발표하면서, Trusted Web이란 용어를 사용한 바 있다. Trusted Web은 현재 인터넷/웹의 문제점을 인식하고, Digital ID 관리 중심의 데이터 검증 영역을 확대한다는 개념으로 정의하고 있다.

세계경제포럼(World Economic Forum)은 2022년 “Earning Digital Trust: Decision-Making for Trustworthy Technologies” 보고서를 통해, 디지털 기술과 서비스, 그리고 이를 제공하는 조직이 모든 이해관계자의 이익을 보호하고 사회적 기대와 가치를 유지할 것이라는 신념으로서 ” Digital Trust” 를 소개하였다. 세계경제포럼의 Digital Trust Framework는 사이버보안, 개인정보 보호, 투명성, 시정 및 감사 가능성, 공정성, 상호 운용성과 안전에 대한 내용을 포함한다.

기존에도 Trusted Web과 유사한 개념으로 Web Trust, Web Service Trust, Web of Trust, Trust seal, Safe Net 등 안전한 웹에 대한 요구를 실현하려는 노력이 있어 왔다.

웹의 패러다임 변화(Web 3.0)와 AI, 블록체인, 메타버스 등 새로운 기술과의 결합을 통한 웹서비스의 변화에 따라, 사이버보안, 개인정보 보호, 투명성, 공정성, 상호 운용성, 감사 및 추적 등이 가능한 안전한 인터넷/웹(가칭, Trusted Web)에 대한 기본 개념을 정의하고자 한다.

Trusted Web에 대한 개념을 정의하기 위해, 일본 내각관방의 Trusted Web, 세계경제포럼의 Digital Trust, DID 기반 Trusted Framework 도구 개발 및 컨설팅 회사인 Mattr의 개념을 도입하여 재구성 하였다. 특히, 앞 절에서 언급한 현 인터넷/웹의 문제점을 극복하기 위한 방안으로서의 Trusted Web에 중점을 두고자 하였다.

### 1. Trust Framework

트러스트 프레임워크는 네트워크 또는 생태계를 구성하는 다양한 이해관계자를 위한 관행과 원칙이다. 트러스트 프레임워크는 이해관계자 및 참가자, 규칙, 승인과 인증, 거버넌스의 4가지 요소로 구성된다.



### 1.1. 이해관계자 및 참가자(Stakeholders, Participants)

Trusted Web에서 "Stakeholder(이해관계자)"는 해당 웹 환경에 영향을 미치거나 영향을 받을 수 있는 모든 관계자를 의미한다. 이는 사용자, 서비스 제공자, 개발자, 정부기관, 규제기관, 그리고 기타 관련 이해관계자를 포함한다. Trusted Web은 이러한 다양한 이해관계자들의 요구와 기대를 고려하여 안전하고 신뢰성 있는 웹 환경을 제공하는 것을 목표로 한다.

한편, Participant(참가자)는 Trusted Web 프레임워크에 활동적으로 참여하는 주체로 정의된다. 이는 특정 웹 생태계나 네트워크에 참여하고 있는 모든 주체를 포함하며, 발행자, 보유자, 주체, 신뢰 당사자, 서비스 및 인프라 제공자 등 다양한 역할을 맡을 수 있다. Trusted Web은 참가자들 간의 상호작용에서의 안전성과 신뢰성을 유지하고 강화하기 위해 규칙과 인증 프로세스를 정의한다.

### 1.2. 규칙(Rules)

규칙은 프레임워크에 참여하는 모든 이해관계자를 인증하는 기준과 표준을 나타낸다. 규칙은 Trusted Web의 안전성과 신뢰성을 유지하기 위한 핵심 원칙을 정의하고, 이를 준수하는 참가자들을 식별한다.

규칙은 Trusted Web의 안전한 아키텍처를 유지하면서 모든 참가자가 일관된 표준과 규정을 따르도록 보장한다. 이를 통해 웹 환경에서의 데이터 처리, 사용자 인증, 서비스 제공 등이 신뢰성 있고 투명하게 이루어지도록 하며, 거래 불공정성 및 보안 위협으로부터 사용자와 다양한 이해관계자를 보호하는 것을 목표로 한다.

### 1.3. 승인과 인증(Accreditation and Authentication)

Accreditation은 특정 참가자가 Trusted Web 환경에서 신뢰할 수 있는 주체로 인정되도록 하는 절차를 말한다. 이는 참가자의 능력, 신뢰성, 보안수준 등을 평가하여 인증하는 과정을 포함한다. Accreditation은 참가자들 간의 균형된 신뢰를 구축하고 유지하기 위해 중요한 단계로 작용한다.

Authentication은 참가자나 사용자의 신원을 확인하고 검증하는 프로세스를 의미한다. Trusted Web에서는 사용자와 다른 참가자들 간 상호작용할 때, 상호간 주장하는 신원을 입증하고 검증할 수 있도록 하는데 주력한다. 이를 통해 신뢰할 수 있는 참가자와 안전한 트랜잭션을 유지함으로써 Trusted Web 환경의 보안성을 강화하도록 한다.

Accreditation과 Authentication은 Trusted Web에서 안전하고 신뢰성 있는 거래 및 정보 전달을 지원하기 위한 핵심 요소로 작용한다.

#### 1.4. 거버넌스(Governance)

거버넌스(Governance)는 Trusted Web 환경의 운영, 관리, 규제, 정책 결정을 책임지는 프로세스와 기관을 나타내며, Trusted Web 프레임워크 내에서 시스템이나 생태계의 적절한 기능과 규칙을 수립하고 유지하는데 중점적인 역할을 수행한다.

거버넌스는 Trust Framework를 필요에 따라 검토하고 업데이트하며, 참가자들 간의 상호작용에서 발생하는 문제를 해결할 책임을 가진다. 또한, 거버넌스는 트러스트 프레임워크의 적용과 실행에 관한 지침을 제공하고, 정책수립 및 규제를 담당하여 Trusted Web이 안전하고 효과적으로 운영되도록 보장한다.

## 2. Trusted Web

Trusted Web은 보안, 데이터 신뢰성, 사용자 신뢰성 강화를 통한 안전한 웹 생태계(Ecosystems)를 말하며, 다음과 같은 핵심기능을 수행한다.

### 2.1. Trusted Web 특성

Trusted Web은 신뢰할 수 있는 웹 환경을 만들기 위한 다양한 기술 및 접근 방식을 가지며, 일반적인 특성은 다음과 같다.

- o 보안과 개인정보 보호: 사용자의 개인정보를 보호하고 보안문제에 대처하기 위한 강력한 보안기능을 갖춘다.
- o 신뢰성 있는 콘텐츠: 가짜뉴스, 사기성 웹사이트 및 해로운 콘텐츠로부터 사용자를 보호하기 위한 방법으로써 사용자에게 정확하고 신뢰할 수 있는 정보를 제공한다.
- o 사용자 중심 설계: 사용자 경험을 중시하며, 사용자가 특정 플랫폼에 종속되지 않도록 분산형 아키텍처를 구성한다.
- o 투명성과 규정 준수: 운영 및 데이터 수집과 관련된 프로세스에 대해 투명성을 유지하고, 관련 규정 및 법률을 준수한다.
- o 신뢰할 수 있는 인증 및 식별: 웹사이트 및 서비스는 사용자의 신원을 확실하게 확인하고, 사용자를 안전하게 식별하기 위한 강력한 인증 메커니즘을 구현한다.

## 2.2. Trusted Web 구성 요소

### 2.2.1. 송·수신정보 인증(Information Authentication)

웹 상에서 교환되는 정보의 신원을 확인하고 보증하는 과정을 의미한다. 이 기능은 정보의 송신자와 수신자가 신뢰할 수 있는 주체임을 검증하고, 정보가 중간에 변조되지 않았음을 보장하기 위한 것이다.

송·수신정보 인증은 전자서명, 암호화, 디지털 인증서 등의 기술을 활용하여 정보의 무결성을 보호하고 송신자의 정당성을 입증한다.

### 2.2.2. 데이터 신뢰(Data Trust)

웹 상에서 교환되는 데이터에 대한 신뢰성 보장을 의미한다. 이는 데이터의 원본이나 진정성을 확인하며, 데이터가 중간에 변경되거나 위조되지 않았음을 보장하는 프로세스를 말한다.

데이터신뢰는 데이터의 무결성 검사, 디지털 서명을 통한 진본성 검증, 데이터 암호화를 통한 유출방지, 안전한 전송 데이터 프로토콜 등 보안기술을 활용하여 보장한다.

### 2.2.3. 자격증명(Credential)

특정 사용자나 참가자가 자신의 신원을 입증하는 수단이나 정보를 말한다. 이는 사용자가 해당 웹 환경에서 누구인지를 확인하고, 신뢰할 수 있는 주체로 인증하는 데 사용된다.

자격증명은 주로 디지털 형태로 제공되며, 사용자의 ID와 비밀번호, 바이오 정보, 디지털 서명 등 다양한 인증수단을 포함한다. 자격증명을 통해 사용자의 신원을 확인하고 보안수준을 유지함으로써 안전한 상호작용을 지원한다.

자격증명은 객체정보(Identity Information)와 객체의 속성(Attribute)들로 구성되며 디지털 ID와 결합하여 신뢰체인을 생성하고, 고유한 컨텍스트를 전달할 수 있도록 하여 새로운 유형의 확장성을 생성한다. 자격증명의 검증요소는 다음과 같다.

- 객체정보: 성명, 고유정보, 그 밖의 증명 정보
- 속성정보: 역할, 권한, 자격증, 거래 권한 등
- 디지털 서명: 신원 및 데이터의 고유성 증빙
- 유효기간: 크리덴셜의 유효기간
- 발행자 정보: 기관명, 연락처, 인증기관 등
- 접근권한: 거래 또는 접근 시스템에 대한 허가

#### 2.2.4. 데이터 추적(Data Tracking)

웹을 이용하는 모든 이해관계자 및 참여자를 개체로 보고, 개체의 활동과 접근기록은 물론 객체와의 연관성을 기록하고 관리한다.

데이터 추적은 개인정보와 데이터에 대한 주권을 주장하기 위한 근거자료가 된다. 즉, 사용자는 자신의 데이터가 어떻게 수집되고 활용되는지에 대한 투명성을 감시하고 관리할 수 있다. 또한, 플랫폼 서비스 사업자와의 공정한 거래를 구현할 수 있다. 이는 사용자와 사업자간의 상호작용에 대한 이해를 토대로 공정한 거래 및 서비스 제공을 보장한다.

#### 2.2.5. 동적동의(Dynamic Consent)

사용자가 개인정보 수집 및 활용에 대한 동의를 유연하게 관리할 수 있는 개념으로, 사용자가 언제든지 자신의 정보제공 범위에 대해 설정하고 변경 및 제어할 수 있도록 하는 원칙을 기반으로 한다. 동적동의는 다음과 같은 특징을 포함할 수 있다.

동적동의는 실시간으로 업데이트되는 동의 상태를 포함하며, 사용자에게 데이터 수집 목적과 수집되는 세부정보에 대해 투명성을 제공한다. 이를 통해 Trusted Web은 개인정보에 대한 과도한 수집과 제공을 통제할 수 있다.

### 2.3. Trusted Web 요소기술

Trusted Web의 특성과 구성요소를 통해, Trusted Web을 구축하기 위한 핵심 기술로 분산형 ID, 분산형 아키텍처, 데이터 추적 및 검증 등이 있다.

#### 2.3.1. 분산형 ID (Decentralized Identity)

중앙 집중형 ID 시스템 대신 블록체인과 같은 분산기술을 기반으로 한 사용자의 신원관리 방식이며, 사용자는 자신의 ID를 중앙기관이 아닌 분산된 레지스터에 저장하고 관리한다.

분산형 ID를 위해 분산된 레지스트리와 디지털 지갑 및 디지털 서명 등의 기술을 활용할 수 있다.

- o 분산된 레지스터: 사용자의 신원 정보는 중앙 집중형 데이터베이스가 아니라 분산된 레지스터에 저장되며, 중앙화된 서버의 취약점을 제거하고, 블록체인과 같은 기술을 사용하여 변경 이력을 투명하게 기록할 수 있다.
- o 디지털 지갑: 사용자는 디지털 지갑을 통해 자신의 신원정보를 안전하게 보관하

고 관리한다. 디지털 지갑은 사용자의 비밀키와 공개키를 기반으로 하여 안전한 서명 및 인증을 제공한다.

- o 디지털 서명: 사용자는 자신의 디지털 지갑을 사용하여 디지털 서명을 생성한다. 디지털 서명은 사용자의 신원을 증명하고, 블록체인과 같은 분산된 레지스터에 기록된다.

### 2.3.2. 분산형 아키텍처 (Decentralized Architecture)

분산형 아키텍처는 중앙 집중형 시스템 대신 데이터와 기능을 여러 노드에 분산시키는 아키텍처로, 높은 신뢰성, 안정성, 확장성을 제공한다. 분산형 아키텍처는 분산 데이터 저장, 분산된 레지스트리, 스마트 계약, 분산된 응용프로그램 실행, 데이터 일관성 및 동기화 등의 기술로 구현될 수 있다.

- o 분산 데이터 저장: 중앙 집중형 데이터베이스 대신 데이터는 여러 노드에 분산 저장되어, 데이터의 가용성을 향상시키고, 단일 지점에서의 데이터 손실을 방지한다.
- o 분산된 레지스터: 데이터 및 서비스에 대한 레지스터가 분산되어 있어 중앙화된 특정 서버의 장애가 전체 시스템에 영향을 미치는 것을 방지한다. 이는 분산형 데이터베이스나 블록체인과 같은 기술을 사용하여 구현될 수 있다.
- o 스마트 계약: 스마트 계약은 계약의 조건이 충족되면 자동으로 실행되는 프로그램으로, 중앙화된 중간단계 없이 계약을 체결하고 이행할 수 있도록 한다.
- o 분산된 응용프로그램 실행: 응용프로그램이 여러 노드에서 병렬로 실행됨에 따라, 성능향상과 시스템의 확장성을 증가시킬 수 있다.
- o 데이터 일관성 및 동기화: 분산된 데이터 저장소 간에 데이터 일관성을 유지하고, 동기화하는 기술이 중요하다. 이를 위해 일관성 있는 해시 함수, 분산 데이터베이스, 블록체인 등이 사용될 수 있다.

### 2.3.3. 데이터 추적 및 검증(Data Traceability and Verification)

데이터의 생성부터 폐기까지의 전 과정을 투명하게 기록하고 검증하는 과정을 의미한다. 이는 데이터의 신뢰성, 무결성, 그리고 데이터 원본의 추적 가능성을 강화하여 사용자에게 신뢰할 수 있는 웹 경험을 제공한다. 주요 기술적 특징은 블록체인, 디지털 서명 및 해시, 분산된 원장, 스마트 계약 등의 기술을 활용할 수 있으며, 분산형 아키텍처와 통합하여 데이터 추적 및 검증의 일관성과 무결성을 확보할 수 있다.

## 제 2 장 국가별 Trusted Web 구축 동향

Trusted Web의 핵심은 사용자의 신원을 확인하고 인증하는데 사용되는 정보나 자격인 크리덴셜에 관한 관리와 활용성이다. 국가별로는 디지털 ID로 표현되는 크리덴셜에 대한 이해관계자의 책임과 역할, 보안 기준 및 규칙 등을 정의하는 “Trust Framework”를 정의하고 있다.

현재 EU, 영국, 미국, 캐나다 등의 국가에서는 국가별 거버넌스 정책에 기반한 Trust Framework를 설계하고 세부 실행 및 구현방안을 논의하고 있다. 여기서는 각국의 Trust Framework에 대한 정책방향과 진행내용에 대해 설명한다.

### 제 1 절 유럽 국가

#### 1. 유럽연합(EU)

##### 1.1. 디지털 ID 정책의 방향

###### 1.1.1. 공통 식별번호, 디지털 ID

EU 전체에 대한 통일적인 식별번호는 존재하지 않으며, 가입국에 따라 다르다. EU 가입국 간 공공 온라인 서비스에 접근할 때 본인인증을 할 수 있는 디지털 ID는 eIDAS(electronic IDentification, Authentic and trust Services)로 2014년부터 규정하고 있다. eIDAS 개정(안)(eIDAS2.0)에서는 모바일 월렛(EUDIW)의 제공을 가입국에 의무화하고, eID를 포함한 속성증명 및 공적문서를 저장 및 이용 가능하도록 하였다.

###### 1.1.2. 트러스트 프레임워크 개발 상황: Regulation 910/2014: eIDAS (2.0)

EU는 전자상거래에 대한 통일된 기준을 마련하기 위해 eID, EUDIW, 및 트러스트 서비스의 법적 효력과 요건을 규정하고 있다. 이는 OIX(Open Identity Exchange)\*2의 Smart Digital ID Trust Frameworks에서도 참조되고 있으며, EU 가입국에 직접 적용되는 법적 강제력을 가지고 있다. 적절한 서비스 제공자를 QTSP(Qualified Trust Service Provider)로 인증하고 EU 가입국 간의 서비스를 상호 인정하도록 하고 있다. 이 규정은 이해관계자의 정의와 요건을 주요하게 다루고 있으며, EUDIW의 제공을 의무화하는 컴포넌트로도 포함되어 있다.

### 1.1.3. 유스케이스

유럽위원회의 노력으로 eSSIF(European Self-Sovereign Identity Framework)-Lab에서는 eSSIF와 관련된 연구와 개발을 진행하고 있다. SSI의 실현을 명분으로 하는 EUDIW의 구현을 위한 파일럿 프로젝트를 실행하고 있으며, 현재까지 개발된 유스케이스는 무역, 의료, 교통, 교육, 소매, 여행, 행정 등 7개의 분야에서 PoC 단계로 진행되고 있다.

### 1.1.4. 정책 방향

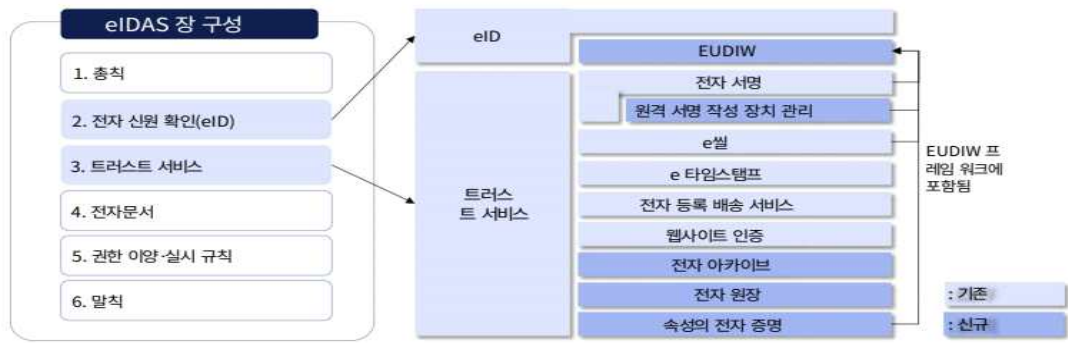
통일적인 식별번호는 없고, 정부는 강제력을 가진 트러스트 프레임워크를 통해 디지털 ID와 관련 서비스, 컴포넌트에 대한 가입국 간의 일정한 상호 운용성을 보장하고 있으며, 인증제도 준수 시 인센티브를 부여하고 있다. 또한, EUDIW나 ESSIF와 같은 개발 프로그램을 실행하여 SSI의 실현을 암시하고, 정부로서 SSI/DID의 실현에 주력하고 있다.

## 1.2. 디지털 ID 추진현황

### 1.2.1. eIDAS 2.0

1999년 제정된 ‘전자서명명령(1999/93/EC)’에서 내용을 추진하여 EU의 전자상거래의 통일된 기준을 마련하기 위해 제정되어 2016년 7월에 고시되었다. 주로 전자 본인인증인 「eID」와 전자서명, e 타임스탬프와 같은 전자 서비스인 「Trust Service」의 요건, 법적 효력, 보안 등에 대해 규정하고 있으며, 트러스트 서비스 사업자인 TSP(Trust Service Provider)는 감독 기관으로부터 평가를 받음으로써 회원국 간 동등한 법적 효력을 얻는 적격 QTSP 인증을 받았다.

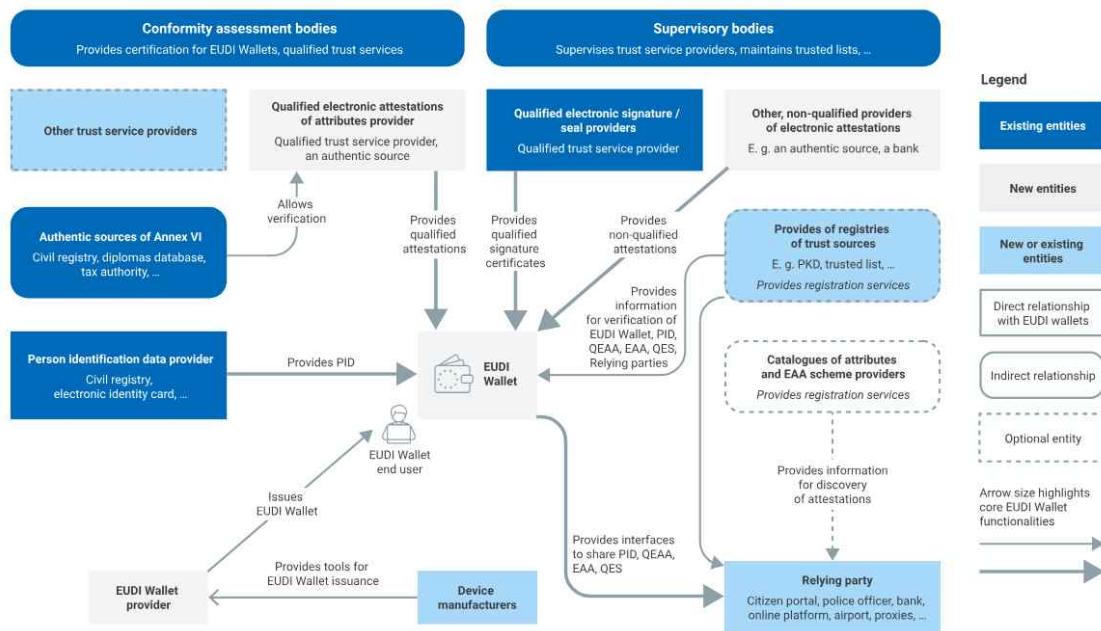
이후 eIDAS 검토 결과 밝혀진 문제점들에 대한 과제(EUDIW 프레임워크 설정, 트러스트 서비스 확대, 하위 규칙 정비, 브라우저 대응 등)를 배경으로 2021년 6월 유럽위원회는 eIDAS 2.0 입법을 제안하였다. 다음 그림은 eIDAS 1.0에서 추가된 신규 분야를 보여준다.



(그림 6) eIDAS 2.0 구성요소

### 1.2.2. EUDIW 생태계

eIDAS 전문가 그룹은 EUDIW 개념에 대한 이해를 촉진하기 위해 ‘EU 디지털 ID 아키텍처 기술 및 레퍼런스 프레임워크’를 공개하고 있다. EUDIW 생태계는 최종 사용자를 중심으로 Identity를 제어하는 구조를 설명한다. 다음 그림은 EUDIW 생태계 구성도를 보여준다.



(그림 7) EUDIW 생태계

### 1.2.3. eID

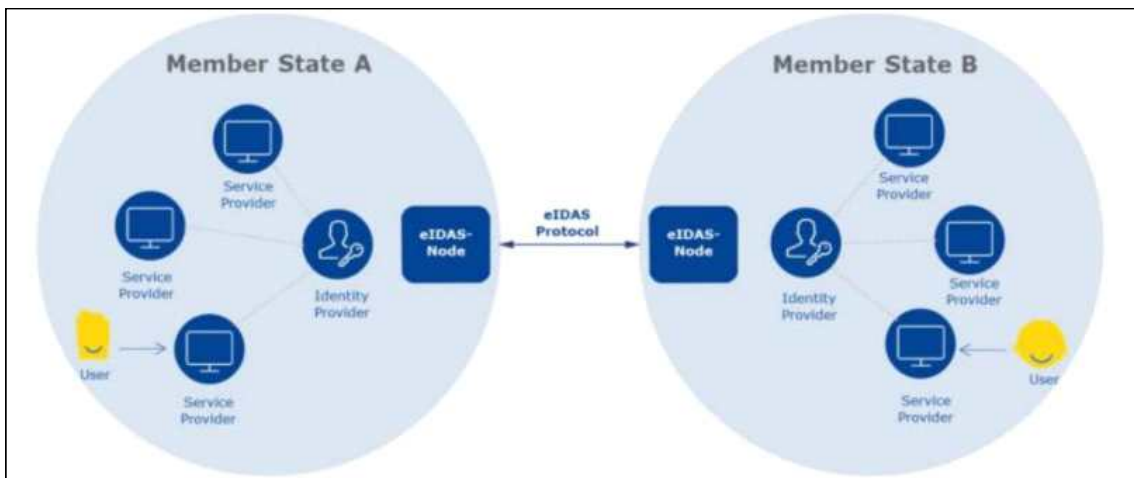
eID는 eIDAS 1.0에 의해서 규정된 EU 회원국 간 공공 온라인 서비스 접속 시 본인 확인을 수행할 수 있는 디지털 ID이며, 회원국은 eIDAS 네트워크에 접속하는 국내 eID 체계를 지정하고 다른 회원국에게 통보함으로써 동료 검토를 받고 상호 승인



을 받아 사용할 수 있다.

각 국가는 eID 사용과 관련된 회원국 간의 통신을 위해 eIDAS 노드를 구현해야 한다. eIDAS 노드는 하위 규칙 CIR(EU) 2015/1501에 그 요건이 규정되어 있지만, 구체적으로 사용하는 기술은 지정되어 있지 않고, 구현을 참조할 수 있는 샘플 소프트웨어만 유럽위원회에서 제공하고 있다.

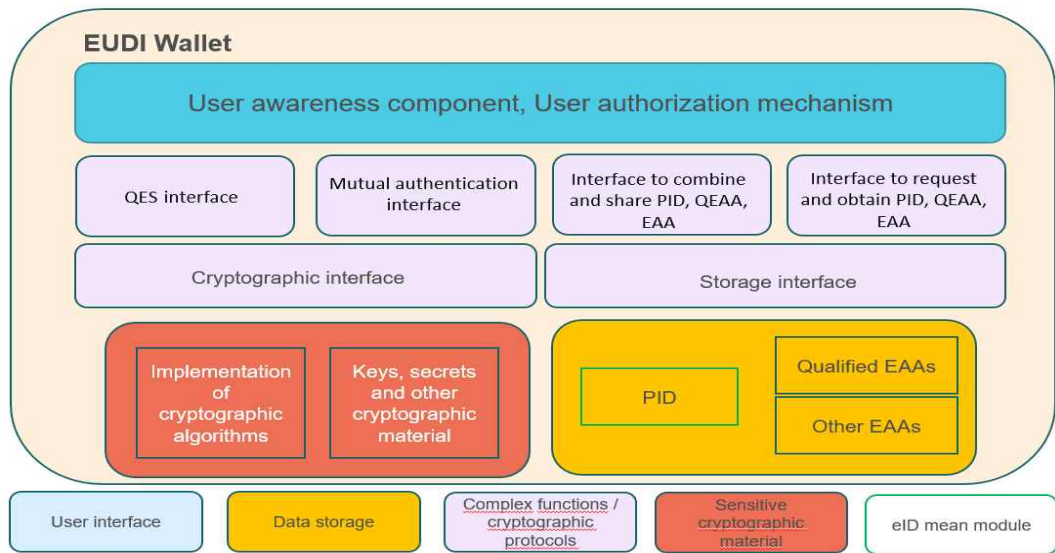
다음 그림은 eIDAS 노드를 통한 회원국 간 eID 사용의 예시를 보여준다. 회원국 A의 시민이 회원국 B의 온라인 서비스를 이용할 때 본인 인증이 요구되고, 회원국 A의 시민은 A의 eID를 가지고 있기 때문에 인증 요청은 회원국 A의 ID 제공자(IdP)에 eIDAS 노드를 통해 전송된다. 인증 결과는 회원국 B의 온라인 서비스 제공자에게 반환되며 인증이 완료되고 시민은 서비스에 대한 액세스를 계속할 수 있다.



(그림 8) eIDAS 노드를 통한 회원국 간 eID 사용 예

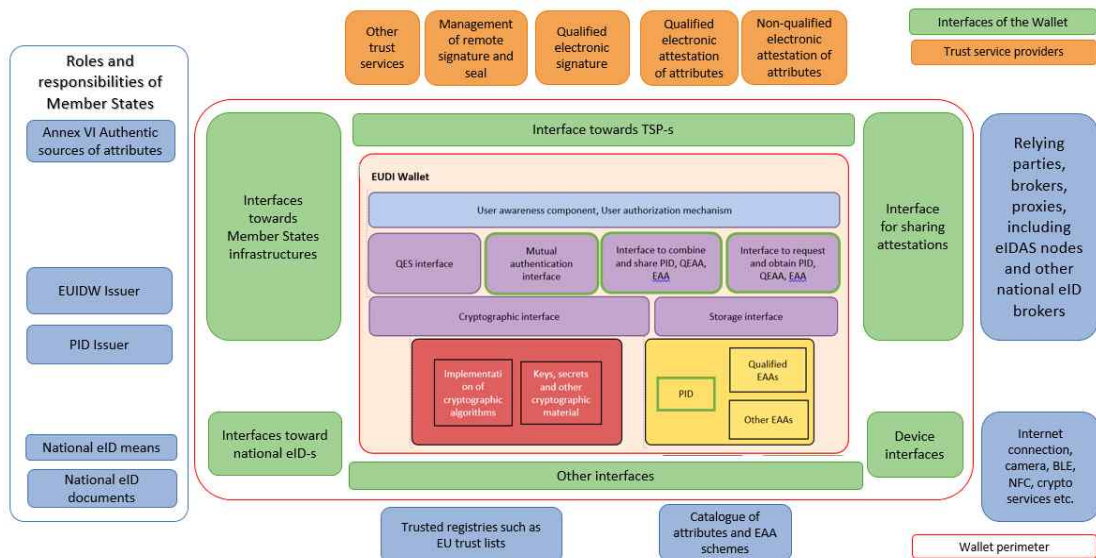
#### 1.2.4. EUDIW

EUDI 월렛의 구성 요소는 사용자 인터페이스, 데이터 저장, 복잡한 기능/암호 프로토콜, 민감한 암호 자료, eID 수단 모듈 등 다섯 가지 범주로 나뉘어 있다. 일부 기능은 EUDIW 자체, EUDIW 하위 시스템 또는 인터페이스를 통해 외부 개체에 의해 제공될 수 있다. QES 인터페이스는 로컬 또는 원격서명 프로세스를 모두 포함할 수 있다. 다음 그림은 EUDI 지갑 기능을 구성요소를 보여준다.



(그림 9) EUDI Wallet 기능

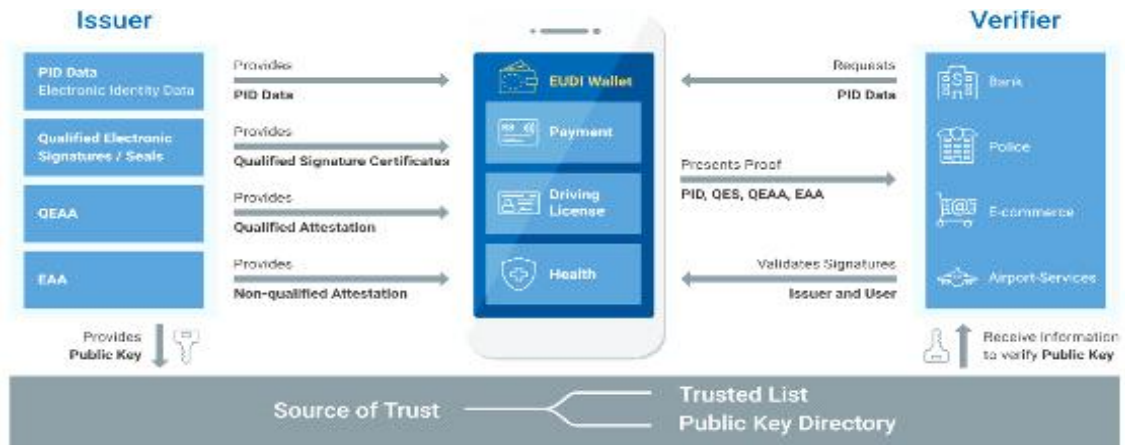
EUDIW는 특정 요구사항, 명세 및 표준이 적용되는 외부 엔티티와의 인터페이스를 포함 한다. 아래 그림은 인터페이스들을 나타내고 있으며, EUDI 지갑의 인터페이스(녹색)는 전용 기술명세서에서 정의된다. 이러한 인터페이스들은 EUDI 지갑 구성요소의 설계에 영향을 미치며, EUDI 지갑 프로토타입의 초기 단계에서 명시한다. QES 인터페이스는 로컬 또는 원격 서명 프로세스를 모두 다룰 수 있다.



(그림 10) EUDI Wallet의 인터페이스

### 1.2.5. eIDAS 2.0 Toolbox

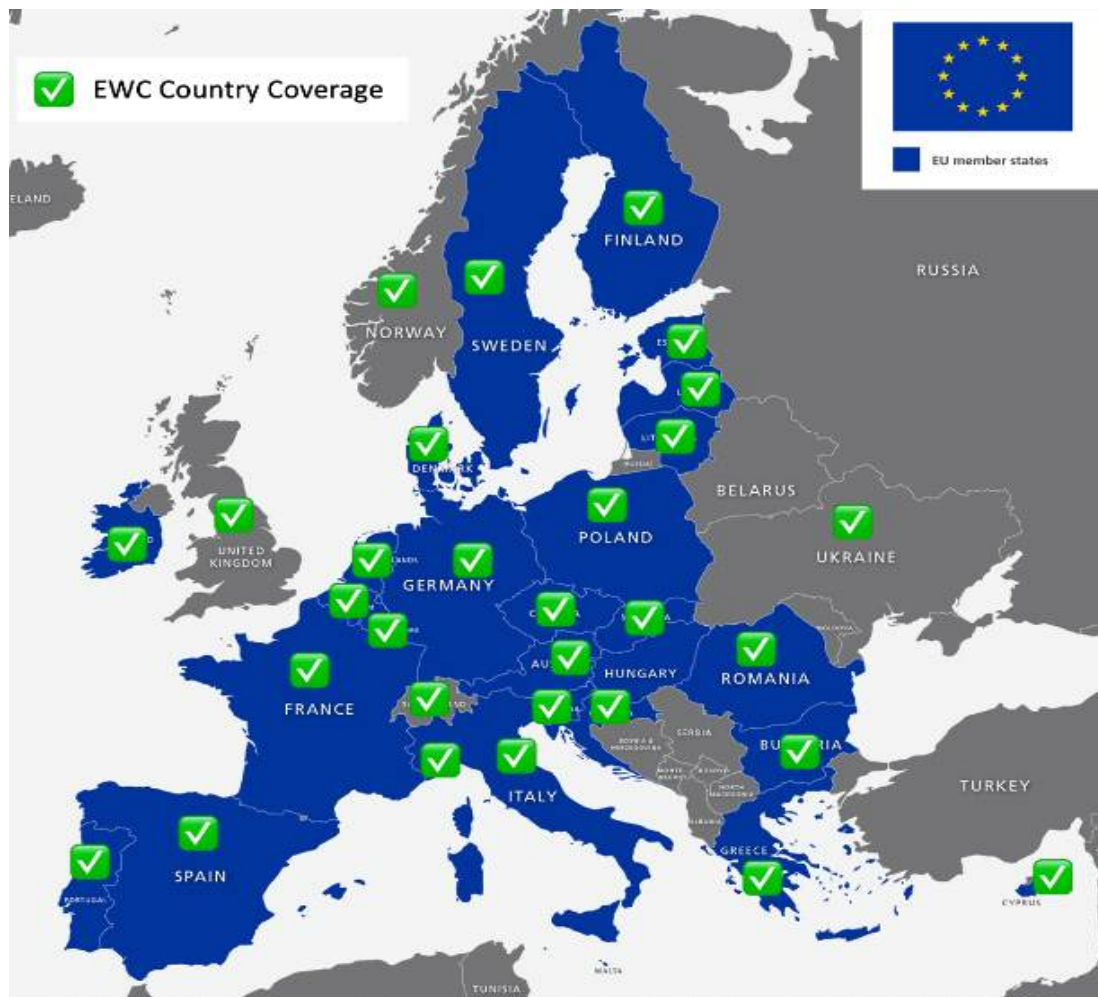
지갑의 기능은 식별 및 인증, 증거성 검증, 검증된 신원 및 그 데이터의 안전한 보관, 전자서명 및 인감생성 등이다. 다음은 eIDAS 2.0 툴박스 구조를 보여준다.



(그림 11) SSI 아키텍처에 매핑된 eIDAS Toolbox

### 1.3. EUDI Wallet 컨소시엄

EU 디지털 월렛 컨소시엄(EWC, EUDI Wallet Consortium)은 제안된 EU 디지털 신분증인 디지털 여행 자격증의 혜택을 회원 국가 전체에 성공적으로 활용하기 위한 EU 회원국 간의 공동 노력이다. EWC는 27개 회원국의 대표로 구성되며 다른 국가의 파트너도 포함된다. 이러한 광범위한 표현은 자연인과 법인 모두에 대해 개인식별 데이터(PID)를 발행할 수 있는 고유한 기능을 제공한다. EWC는 사람들의 온라인 생활에 핵심이 되는 규모가 크고 채택률이 높은 사용 사례에 중점을 두고 있다. 다음 그림에서는 EWC에 참여한 국가를 표시하고 있다.






(그림 12) EWC 참여 국가

유럽위원회는 유럽 시민 및 기업이 신원 데이터를 안전하고 편리하게 공유할 수 있도록, 유럽 디지털 ID 규정에 따라 EU 디지털 신원 지갑(EUDIW)의 프로토타입을 제공할 수 있다.

다음 표는 국가별로 참여한 유스케이스를 보여준다.

[표 3] 국가별 테스트된 유스케이스

국가	시험운영 프로젝트			
				
벨기에	1, 4, 5			
불가리아				
체코공화국	3, 6	9		8
독일	1, 2, 3, 4, 5		10	7, 8, 9
덴마크		9	10, 11	
에스토니아	4			
아일랜드			11	
그리스	1,2,3,4,5,6		10	7, 8
스페인	4, 6		10	7
프랑스	1,2,3,4,5,6			8, 9
크로아티아				
이탈리아	1, 4, 6	9		8
키프로스	1, 4, 5, 6			
라트비아		9		
리투아니아	4		10	
룩셈부르크	1, 2, 3, 4, 5		10	7
헝가리	6			7
몰타			10	
네덜란드	1, 3, 4	9	11	8
오스트리아	1,2,3,4,5,6		11	
폴란드	1, 3, 4, 6			7
포르투갈	1, 2, 4, 5, 6		10, 11	
루마니아			10	9
슬로베니아	1, 2, 5		10	
슬로바키아	1, 4, 5			
핀란드	1, 4			7, 8
스웨덴			10	8, 9
노르웨이		9	10	8
아이슬란드		9		
스위스				7
우크라이나	1,2,3,4,5,6			9

1. 정부서비스 접근: 여권, 운전면허증, 세금신고, 사회보장정보 접근 등 공공 서비스 접근  
2. 은행계좌 개설: 온라인 계좌 개설 시 본인확인  
3. SIM 등록: 선불 및 후불 SIM 카드 계약(등록 및 활성화)을 위한 신원 증명  
4. 모바일 운전 면허증: 온·오프라인에서 모바일 운전 면허증을 저장하고 제시하는 것  
5. 계약서 서명: 온라인 계약서 서명을 위한 안전한 디지털 서명을 생성  
6. 처방전 청구: 약국에 처방전 세부정보를 제공, 의약품 조제  
7. 여행: 여행 서류(예: 사용자의 여권, 비자 등)의 정보를 제시  
8. 조직 디지털 신원: 귀하가 조직의 합법적인 대표자임을 증명  
9. 결제: 온라인 결제 시 사용자의 신원 확인  
10. 교육 증명서: 졸업장, 학위, 증명서 등 교육 자격 증명의 소지 증명  
11. 사회보장 혜택 이용: 퇴직 또는 장애 혜택 등 사회보장 정보 및 혜택에 접근

## 2. 독일

### 2.1. 디지털 ID 정책의 방향

#### 2.1.1 공통 식별번호, 디지털 ID

각 행정 분야마다 다른 개인 식별번호를 사용하고 있지만, 2021년 4월에 공포된 등록 현대화법에 따라 일정한 제약조건 하에서 세금 식별번호를 전반적으로 활용할 수 있는 시스템 구축이 진행되고 있다. eID 카드가 2010년부터 도입되어 있으며, 16세 이상의 독일 국민에게 취득이 의무화되어 있다.

#### 2.1.2. 트러스트 프레임워크 개발 상황: IDunion Network

IDunion Network은 인터넷 상에서 신뢰를 확립하기 위해 기술과 거버넌스를 TCP/IP 스택의 구조에 영감을 받아 4개의 레이어로 정리하였다. 공공 및 민간의 협력으로 작성되었으며, 준수는 자율적이며 인증 등의 체계는 없다. 이해 관계자, 프로세스, 거버넌스가 규정되어 있으며, 블록체인, DLT(Distributed Ledger Technology), DIDs의 구현이 명시되어 있다.

#### 2.1.3. 유스케이스

정부가 주도하는 SSI 파일럿 프로젝트와 Secure Digital Identity 쇼케이스와 같은 프로젝트를 실행하고 있으며, 적극적으로 PoC를 수행하고 있다. 현재까지 개발된 유스케이스는 14건으로 금융, 보험, 의료, 공급망, 교통, 교육, 소매, 여행, 행정 등 9개 분야에서 컨셉 단계 1건, PoC 단계 12건, 실제운영 1건으로 정부의 지원을 받아 활발히 진행되고 있지만 현재 대부분이 PoC 단계에 있다.

#### 2.1.4. 정책 방향

개인정보 보호를 위해 통일적인 식별제도는 가지고 있지 않고, 국내에서 상호 운용성 있는 디지털 ID(eID 카드)를 운영하고 있다. 트러스트 프레임워크는 존재하지만, IDunion 내에서 선택적으로 참조되는 것으로 법적인 강제력은 없으며, 인증제도 등의 준수에 대한 인센티브는 마련되어 있지 않다.

SSI를 실현하기 위한 파일럿 프로젝트에서 PoC를 적극적으로 실시하고 있으며, SSI/DID의 실현에 정부 차원에서 노력하고 있다

## 2.2. 디지털 ID 추진현황

독일은 프라이버시 침해 우려 등의 이유로 국민공통번호를 도입하지 않았고, 행정 분야마다 서로 다른 공통식별번호(조세식별번호나 의료피보험자번호 등)를 이용하여 행정절차가 수행되고 있다.

### 2.2.1. 관련 법규

#### o 등록 현대화법

- 2021년 4월에 고시된 독일 법률로 온라인 액세스법의 개정 및 ID 번호법의 제정에 대해 규정
- 2017년에 제정된 온라인 액세스법에 따라 연방 정부와 주정부는 2022년 말까지 행정 포털 사이트를 통한 행정서비스의 전자적 제공을 의무화

#### o 개정 온라인 액세스법

- 기존의 세무 식별번호를 활용하여 법적 근거 또는 본인의 동의가 있는 경우에 공적 기관간의 데이터 교환을 가능하게 함과 동시에 데이터 보호의 관점에서 데이터 컨트롤 타워를 도입하는 내용 등이 규정
- 데이터 컨트롤 타워는 본인이 자신의 데이터에 대해 어느 기관이 어떤 데이터 요소를 어떤 목적으로 처리했는지 인터넷으로 확인할 수 있는 것으로 특정 개인정보의 제공 상황을 확인할 수 있는 정보 제공 등의 기록 시스템
- 온라인 액세스법은 연방 정부, 주정부 및 지방 자치 단체가 575개의 관리 서비스를 온라인으로 제공하도록 규정

#### o ID 번호법

- 행정 절차상의 데이터를 특정 자연인에게 할당, 데이터 품질향상을 실현, 공적 기관 보유 데이터를 반복해서 다시 제출하지 않도록 하는 것을 목적으로 제정

### 2.2.2. eID 카드

독일에서는 디지털 인증 수단으로 eID 카드가 2010년에 도입되어 16세 이상의 독일 국민들에게 취득이 의무화되어 있다. 공통식별번호와는 관련이 없기 때문에 공통식별제도와 디지털 ID는 별개로서 대처되고 있다.

2017년 연방법 개정으로 eID 카드 발급시 전자 서명 기능을 부여할 수 있다. 등록 현대화법에 의해 정비되고 있는 행정 서비스 온라인 포털 사이트에서도 eID 카드를 이용한 본인 인증 기능을 사용할 수 있다.

### 2.3. IDunion

IDunion 조직의 목표는 전 세계적으로 사용할 수 있고 유럽의 가치와 규정을 기반으로 하는 분산형 ID 관리를 위한 개방형 생태계를 만드는 것이다. 모든 사람(자연인, 법인 및 사물 포함)은 자신의 신원 정보를 스스로 관리하고 이 정보를 누구와 공유할지 결정할 수 있다.

자신의 데이터에 대한 주권은 매우 중요하며, 특히 매우 민감하고 개인적인 정보의 경우 더욱 그렇다. 사용자는 필요에 따라 자격 증명을 저장하고 제3자에게 제공하는 데 사용되는 여러 지갑 중 하나를 선택할 수 있다. 이는 광범위한 사용 사례에 도움이 되며 새로운 ID 관리 방식을 가능하게 한다.

따라서 기술 회사는 더 이상 중앙 ID 관리자가 아닌 사용자 자신의 역할을 수행한다. 사용자는 정보를 볼 수 있는 위치, 정보 관리에 사용되는 프로그램, 이 정보를 누구와 공유할지 결정할 수 있다. 이 개념은 ‘자기주권적 정체성’이라고 할 수 있다.

IDunion 네트워크 구현의 핵심 측면은 보안, 비용 효율성, 사용자 친화성 및 현재 데이터 보호 규정을 준수하는 ID 데이터 사용이다. 목표 중 하나는 잠금 효과를 방지하고 항상 사용자에게 선택권을 제공하는 것이다.

따라서 단일 공급자에 대한 종속성을 만들지 않고도 여러 공급자를 사용할 수 있다. 이는 데이터의 이동성과 다른 국제 네트워크와의 호환성으로 인해 가능하다.

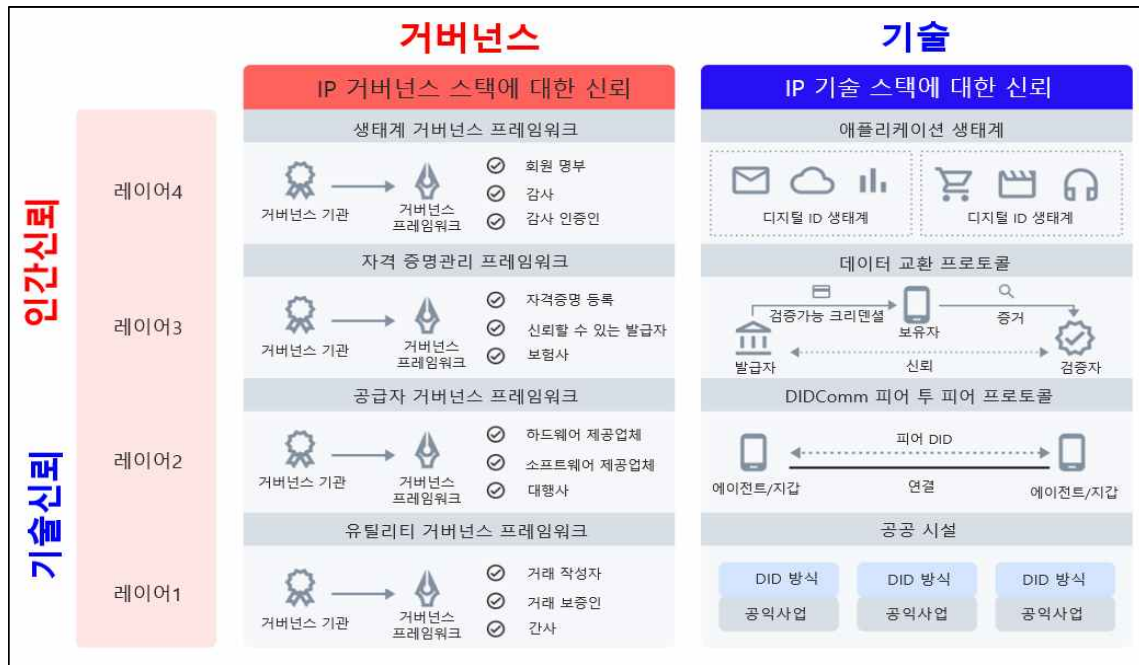
인프라는 기존 기술 표준을 기반으로 하며 유럽 단일 시장 내에서 ‘자기주권적 정체성’의 사용을 허용한다. 분산형 구조, 신원 데이터의 자체 관리, 사용자에게 의한 데이터의 선택적 공개, 유럽의 네트워크 노드 운영은 특히 중요한 데이터 보호 권리와 데이터 경제 지침을 보장하고 개선할 것이다.

사용자는 항상 SSI(자기주권신원) 솔루션의 중심에 있다. 신원 정보 발행자는 네트워크에 공개 식별자를 쓸 수 있다. 정보 검증자는 공개적으로 읽을 수 있는 데이터베이스를 확인하여 수신된 정보가 실제로 해당 발신자로부터 온 것인지 아니면 제3자에 의해 검증되었는지 확인할 수 있다. 솔루션은 자연인과 법인, IoT 모두에 동일하게 적합하다.

IDunion 네트워크는 Trust over IP (ToIP) 모델에 기반하며, 네개의 연속계층으로 구분한다. 첫 번째 계층은 IDunion 네트워크 또는 유사 네트워크이다. 두 번째 계층은 개별 에이전트간의 통신을 다룬다. 이 두 계층이 함께 기술적 신뢰를 형성한다. 세 번째 계층은 개별 역할(발급자, 소지자, 검증자) 및 그들 간의 연결을 설명한다. 네 번째 계층은 금융 산업, 모빌리티, 건강 또는 공공 서비스와 같은 사용 사례를 위한 특정 생태계를 처리한다. 세 번째와 네 번째 계층이 함께 사회적 신뢰를 가능하게 한다.



다음 그림은 IDunion의 구성요소를 보여준다.



(그림 13) IDunion 구성요소: 사용된 기술 및 표준

IDunion은 신원 네트워크 및 에이전트 개발을 위해 국제 표준을 사용한다. 핵심 구성 요소는 다음과 같다.

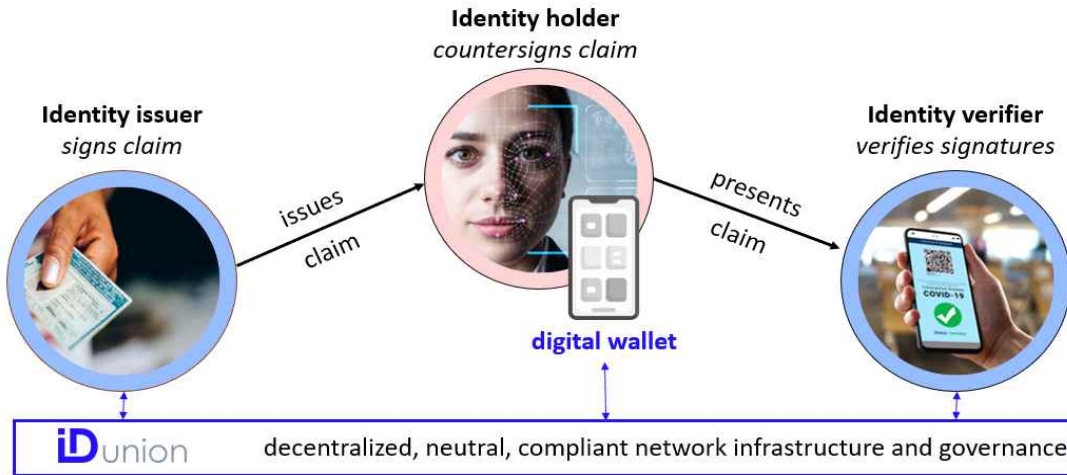
- o World Wide Web Consortium (W3C)에서 지정한 검증 가능한 자격증명 (Verifiable Credentials).
- o W3C에서 제안한 분산 식별자(DID)로, anywise 및 peerwiseDID 사용.
- o Decentralized Identity Foundation (DIF)에서 지정한 DIDcomm메시징 프로토콜로, 에이전트 간 통신에 사용

## 2.4. Self-Sovereign-Identity (SSI)

SSI는 식별된 자연인과 관련된 정보를 설명하는 데이터를 제어하는 기술적 접근 방식을 나타낸다. 신분증, 운전면허증, 학위와 같은 정보에 대한 데이터를 제어하고 법인 엔티티가 탄소 발자국과 같은 제품을 위한 자격을 발급할 수 있도록 한다.

다양한 중앙 플랫폼에 개인 데이터를 제공하는 대신 사용자가 SSI 지갑에서 VCs(Verifiable Credentials)를 사용하여 스스로 인증하고 승인함으로써 플랫폼이나

기타 주체에게 요청 시 제시할 수 있도록 한다. 기본 기능과 일반적인 프로세스 단계는 다음 그림에서 확인할 수 있다.



(그림 14) SSI 기술을 사용하여 자격증명을 확인하는 일반 프로세스

### 3. 영국

#### 3.1. 디지털 ID 정책의 방향

##### 3.1.1. 공통 식별번호, 디지털 ID

예전에는 통합 국민식별번호가 있었거나 검토되었지만 폐지되었다. 현재는 사회 보장, 의료 등 각각의 목적에 따라 다른 식별 번호를 사용하고 있다. 민간 IdP를 행정 서비스에 활용하는 GOV.UK Verify는 2016년 5월 본격적인 운영을 시작했지만, 사업자들의 탈퇴가 잇따라 2023년에 폐지 예정이다.

영국은 The UK digital identity and attributes trust framework를 마련하여 디지털 ID를 상호 운용할 수 있도록 일련의 규칙을 규정하고 있다.

##### 3.1.2. 트러스트 프레임워크 개발 상황: The UK Digital Identity and Attributes Trust Framework

영국에서는 개인 및 개인정보를 증명할 수 있는 서비스를 보다 간편하고 안전하게 사용할 수 있도록 디지털 ID 및/또는 속성정보를 제공할 때 준수해야 할 일련의 규칙이 규정되어 있다. 정부가 주도하여 작성되었으며, 이에 따르는 것은 선택 사항이지만, 프레임워크에 참여를 희망하는 조직은 인증을 받아야 한다. 이해관계자 프로세스를 규정하며, W3C, OIDF 등의 표준을 참조한다.

### 3.1.3. 유스케이스

정부는 SSI/DID 관련 노력과 실증환경을 제공하고 있다. 예를 들어, FCA의 규제 샌드박스와 NHS Digital Staff passport 등이 있다. 현재까지 개발된 유스케이스는 5건으로 금융, 부동산, 의료, 엔터테인먼트 등 4분야에서 컨셉 단계 0건, PoC 단계 3건, 실제운영 2건을 진행하고 있으며, 정부의 지원을 받아 활발히 진행되고 있고 주로 PoC 단계와 실제운영 단계에 있다.

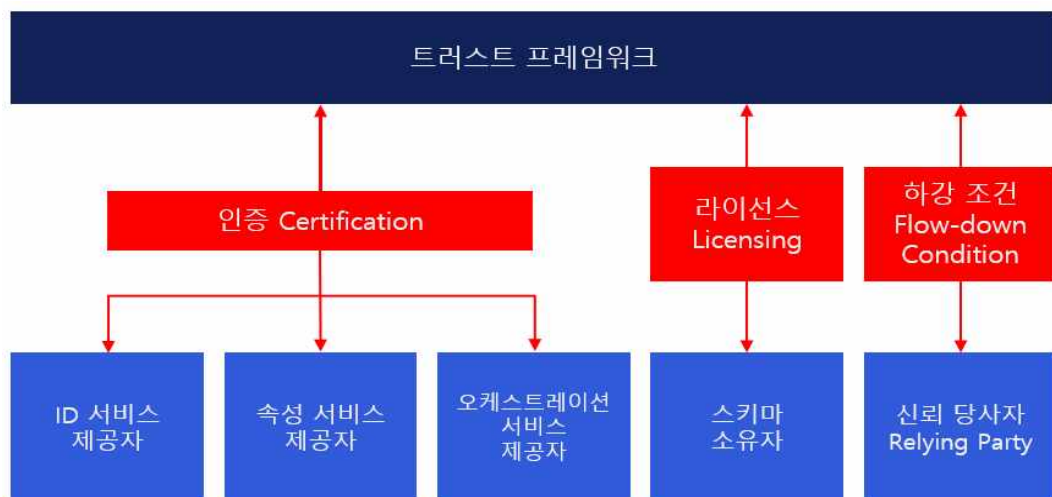
### 3.1.4. 정책 방향

개인정보 보호를 위해 통일된 식별 번호는 제공하지 않고, 관공서에서 상호 운용성이 있는 디지털 ID를 활용하고 있다. 트러스트 프레임워크에 법적인 강제력은 없지만, 준수함으로써 인증을 받을 수 있기 때문에 일정한 인센티브가 제공된다. 정부는 금융, 의료 등의 분야에서 SSI/DID에 관련된 노력을 추진하고 있다.

## 3.2. 디지털 ID 추진현황

### 3.2.1. 트러스트 프레임워크 알파 v2(0.2)

트러스트 프레임워크 알파는 안전하고 신뢰할 수 있는 디지털 ID 및/또는 속성 솔루션을 제공하려는 조직이 따라야 할 규칙 세트를 정의한다. 다음 그림은 트러스트 프레임워크와 구성요소간의 관계를 보여준다.



(그림 15) 트러스트 프레임워크와 구성요소간의 관계

프레임워크에서 선택한 역할은 어떤 신뢰 프레임워크 규칙이 적용되어야 하는지와

인증이 필요한지에 영향을 미친다. 조직이 여러 역할을 수행하려면 각 역할에 대한 규칙을 따라야 한다.

인증을 받으려면 독립적인 인증기관에서 수행하는 역할의 모든 규칙을 따르는지 확인해야 한다. 인증 및 승인 후 신뢰 표시를 받을 수 있다. 이를 통해 다른 조직들이 규칙을 준수하는 것을 확인할 수 있으며, 사용자가 제품이나 서비스를 사용하는 데 더욱 자신감을 가지게 된다.

#### ○ ID 서비스 제공자

- ID서비스 제공자는 사용자의 신원을 증명하고 검증
- 특정 부분에서 사용할 수 있는 구성 요소를 설계하고 구축하는 것에 특화

#### ○ 속성 서비스 제공자

- 속성을 수집, 생성, 확인 또는 공유하는 개인 또는 조직

#### ○ 오케스트레이션 서비스 제공자

- 참여자 간에 데이터를 안전하게 공유 할 수 있도록 기술 인프라 제공

#### ○ 스키마 소유자

- 스키마를 만들고 운영하며 규칙을 설정하는 조직

#### ○ 신뢰 당사자

- 신뢰 프레임워크 참가자의 제품이나 서비스를 사용하는 조직

#### ○ 하강조건(Flow-down Condition)

- 상위 계약 또는 계약 당사자가 특정 조건이나 요구사항을 충족하기 위해 하위 계약자에게 적용할 것을 요구하는 경우에 사용
- 상위 계약에서 지정한 조건이나 표준을 하위 계약자에게 적용하고 요구하며, 하위 계약에 “플로우-다운(flow-down)” 되어 적용
- 계약간에 의무 및 책임을 정의하고 계약자 간의 협력을 강화하기 위해 사용

### 3.2.2. 프레임워크 참여자의 혜택

프레임워크 참여자는 다음과 같은 3가지 혜택을 받을 수 있다.

- 데이터 침해, 신원도용 및 남용에 대한 대응
- 타국가, 타사업, 타기관과 디지털 ID 및 속성 공유
- 데이터 보호와 같은 규정 준수

## 제 2 절 아메리카

### 1. 미국

#### 1.1. 디지털 ID 정책의 방향

##### 1.1.1. 공통 식별번호, 디지털 ID

기존의 사회보장번호(SSN)가 개인 인증에 광범위하게 사용되어 행정 및 민간 서비스 양쪽에서 사용 범위가 확대되었다. 개인정보 보호 등의 우려로 인해 사회보장번호를 대신할 통일된 공통 식별 번호를 모색하고 있지만, 아직 실현되지 않았다.

NSTIC(National Strategy for Trusted Identities in Cyberspace), IDIA(Identity for All) 법안 및 NIST(National Institute of Standards and Technology)의 표준 등으로 정부로서의 디지털 ID 이용 방침을 보여주며, 에코시스템의 형성과 인프라 구축을 추진하고 있다.

##### 1.1.2. 트러스트 프레임워크 개발 상황

###### o IDEF(Identity Ecosystem Framework)

- 미국 정부는 Identity 생태계를 구축하기 위해, 참여 주체의 역할과 필요한 액션, 프라이버시·보안 등의 요건을 정의

###### o NIST SP 800-63-3, SP 800-63-4

- 디지털 ID 서비스를 활용하는 정부 기관을 위한 가이드라인이지만 민간에서도 임의로 참조
- 디지털 인증에서 사용하는 등록·검증의 프로세스에 중점적

##### 1.1.3. 유스케이스

사회보장번호를 대체하는 분산형 식별자(DID 등)를 구현하는 개발 프로그램에 대한 지원이나, 각 주에서의 자주권 ID 구현, mDL 도입 등 SSI/DID에 관한 노력이 연방 정부와 주정부의 주도로 실행되고 있다.

현재까지 개발된 유스케이스는 3건으로 교통, 금융, 의료 등 3개 분야에서 컨셉 단계 0건, PoC 단계 1건, 실제운영 2건으로 정부의 지원을 받아 진행되고 있고 주로 실제운영 단계에 있다.

## 1.2. 정책 방향

SSN은 현재 실질적인 통일적인 식별제도로 사용되고 있지만, 개인 정보 보호 및 정보 유출에 대한 우려로 인해 개선이 추진되고 있다. NSTIC, IDIA 등의 법률과 NIST의 표준을 통해 정부는 디지털 신분증 활용 방침을 제시하고 있으며, 민간 기업들도 이를 참고할 수 있게 되었다. 연방 정부와 주 정부 모두 SSI/DID와 관련된 지원 및 노력을 진행하고 있다.

## 2. 캐나다, Pan Canadian Trust Framework (PCTF)

### 2.1. 디지털 ID 정책의 방향

#### 2.1.1. 공통식별번호, 디지털 ID

사용되는 목적별 식별 번호와 통일된 국민 ID 카드를 발급하는 제도가 일시적으로 검토되었지만, 개인정보 보호 등의 우려로 실현되지 않았다. DIACC가 이끄는 정부 및 민간 기업으로 구성된 비영리 조직에서, 캐나다의 관공서가 디지털 신원을 안전하게 활용하기 위한 거버넌스 모델로 PCTF(Pan-Canadian Trust Framework)를 수립하고 있다.

#### 2.1.2. 트러스트 프레임워크 개발 상황: Pan-Canadian Trust Framework: PCTF

정부와 민간이 함께하는 DIACC에 의해 수립되었으며, 캐나다의 디지털 신원 관리에 대한 이해관계자, 디지털 ID의 작성, 관리, 제공에 관한 일련의 프로세스 등을 정의하고 있으며, 지갑, 인프라 등의 구성 요소도 정의하고 있다. 법적 강제력은 없지만, 선택적으로 참조되고 있으며, Voilà Verified 인증 프로그램을 통해 그 준수에 인센티브를 제공하고 있다. OIX의 Trust Frameworks for Smart Digital ID에서 참조되고 있다.

#### 2.1.3. 유스케이스

ISE에 의한 자금 제공 프로그램이나 ATB Ventures사와의 실증실험, KTDI 참여 등 SSI/DID에 관한 노력은 연방 정부로서 적극적으로 실시되고 있으며, 온타리오 주, BC 주 등 주정부 단위에서도 실시되고 있다. 현재까지 개발된 유스케이스는 4건으로 금융, 의료, 공급망, 교통, 여행, 행정 등 6분야에서 컨셉 단계 0건, PoC 단계 1건, 실제 운영 3건으로 정부의 지원을 받아 진행되고 있고 주로 실제운영 단계에 있다.

#### 2.1.4. 정책 방향

목적별 식별 번호를 사용하여 국민 공동으로 상호 운용성을 가진 디지털 ID를 트러스트 프레임워크로 규정하고 있다. SSI/DID에 관련된 지원·대응을 연방정부·각 주정부 쌍방에서 실시하고 있다.

### 2.2. 디지털 ID 추진현황

#### 2.2.1 Pan-Canadian Trust Framework(PCTF)

디지털 자격증의 생성, 발급, 저장, 제시 및 검증에 참여하는 주체의 진실성, 유효성, 보안 및 개인정보 보호는 해당 자격증의 신뢰성을 평가하는 데 중요하다. 이 PCTF 구성 요소는 디지털 자격증의 신뢰성 평가에 영향을 미치는 주요 신뢰 관계를 식별한다. 이를 고려하여 이 구성 요소에서 식별된 신뢰 관계와 프로세스와 관련된 준수 기준은 관련 당사자 간 신뢰 구축을 위한 기술적 방법 외에도 투명성, 감사 가능성 및 개인 정보 보호에 초점을 두고 있다. 아래 그림은 다양한 역할 간의 관련성 및 이러한 신뢰 관계의 필요성을 보여주는 PCTF의 구성 요소 및 자격증명 역할 및 관계 등의 예시를 제공한다.



(그림 16) PCTF 구성요소

## 제 3 절 아시아

### 1. 일본

내각관방, Trusted Web 신뢰 프레임워크, 아키텍처, 거버넌스를 추가한 Trusted Web White Paper Ver. 2.0을 2022년 8월에 발간하였으며, 파일럿 프로젝트로 개인 정보 분산 이력 관리, 기업 데이터 분산 관리 등 13개의 유스케이스를 개발하였다.

다음 그림은 Trusted Web이 목표로 하는 방향성을 보여준다.



(그림 17) Trusted Web의 방향성과 목표

현재 인터넷은 검증 가능 영역이 협소하여 상대방에 대한 많은 신뢰가 필요하고, 블록체인 등은 강력한 신뢰 기반으로 특정 기술에 의존적이고 에너지 소비 및 업그레이드 용이성에 한계를 가지고 있다.

따라서 Trusted Web의 목표는 “신뢰” 수준을 제고하는 것이다. Trusted Web의 목표는 연속성, 상호운용성, 업그레이드 용이성을 만족하면서 검증 가능한 영역을 확대하는 것이다.

#### 1.1. Trusted Web 프로토타입

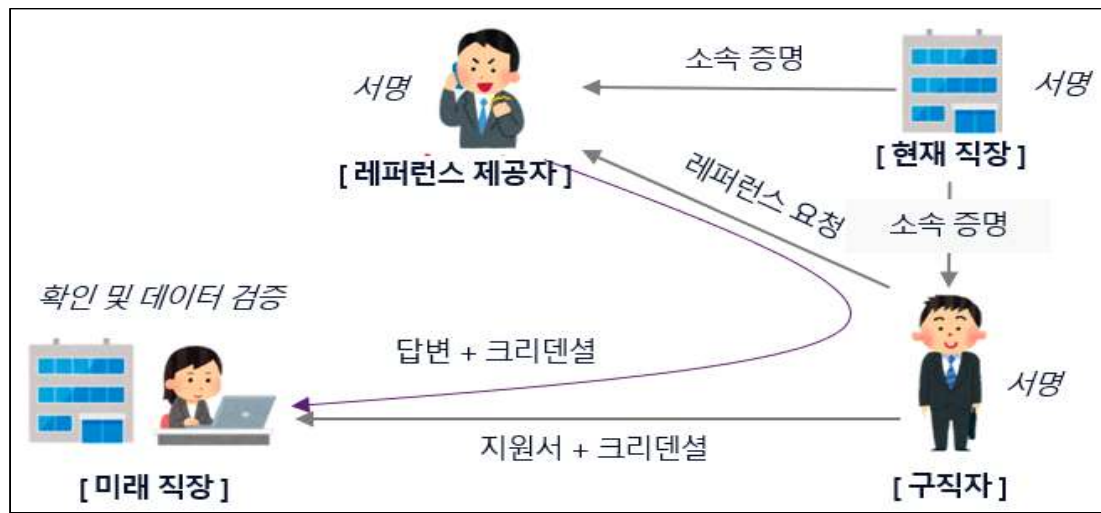
Trusted Web의 기능은 식별자 관리, 신뢰통신, 동적동의, 데이터 추적의 4가지 요소로 구성되어 있다.

- 식별자 관리
  - 사용자는 DID(Decentralized ID)를 발행하고 필요한 데이터를 DID에 연결
- 신뢰통신
  - 데이터 수신시 복호화 가능한 VC(Verify Code) 생성 및 발급자 서명을 검증
- 동적동의



- 데이터 제공자는 필요한 데이터를 스스로 선택하여 임의로 제공
- o 데이터 추적
  - 사용자가 제공한 데이터에 누가 언제 접근 했는지 확인

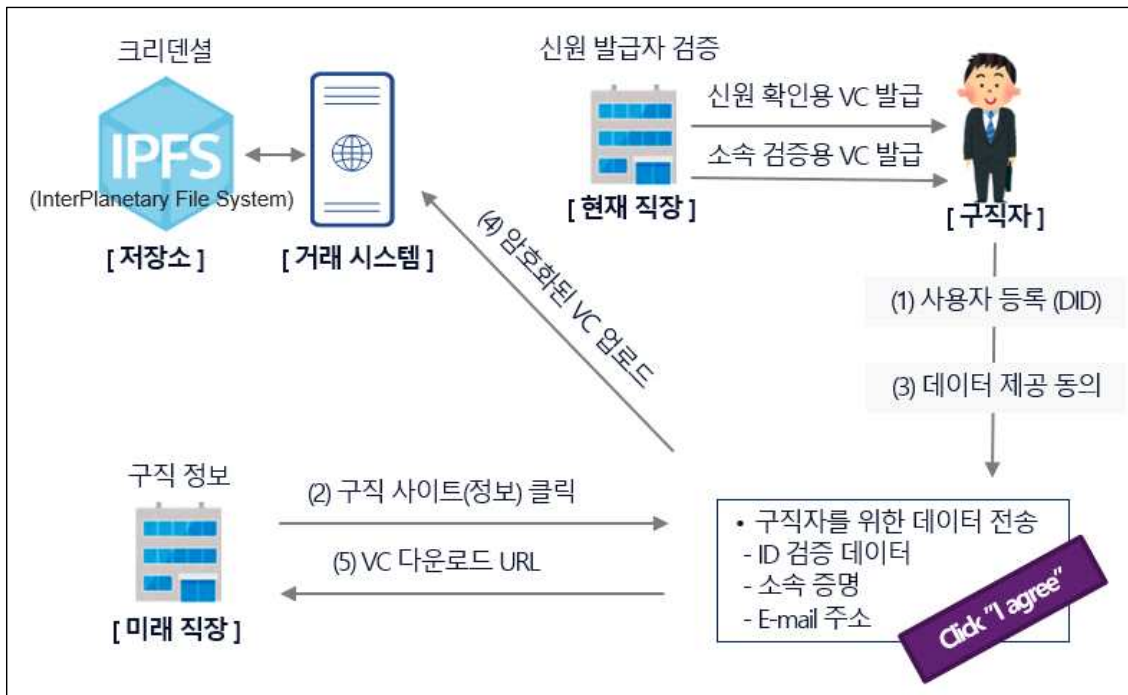
다음 그림은 Trusted Web의 동작과정을 설명하기 위해 구직 사이트와 검증과정을 보여주는 Trusted Web 프로토타입이다.



(그림 18) 구직사이트 Trusted Web 구성도

구직자가 이직을 위해 지원하는 직장에 현재 직장의 소속증명과 크리덴셜을 제출하고, 레퍼런스 제공자가 추가로 크리덴셜과 응답내용으로 이직을 지원하는 직장에 검증을 제공하면 이직을 원하는 직장에서 확인 및 데이터 검증이 가능함을 보여준다.

다음 그림에서는 구직 사이트 프로토타입에서 세부적인 동작 절차를 보여준다. 구직자는 현재 직장(Issuer)에서 신원확인용 VC와 소속 검증용 VC를 발급받는다. 검증자(Verifier)에게 DID로 사용자등록을 하고 데이터 제공에 대한 동의를 한다. 검증자는 구직자에게 받은 ID 검증 데이터와 소속증명, 이메일 주소등을 암호화된 VC로 거래시스템을 통해 저장소에 저장한다. 저장소는 거래 시스템과 저장되어 있는 크리덴셜을 공유한다. 이직을 원하는 직장에서는 거래시스템과 연결되어 있는 구직 사이트에서 정보를 확인하고 VC로 구직을 원하는 구직자의 정보를 확인할 수 있다.



(그림 19) 구직사이트 Trusted Web 동작 절차

## 2. 싱가포르, National Digital Identity (NDI) Stack

### 2.1. 디지털 ID 정책의 방향

#### 2.1.1. 공통식별번호, 디지털 ID

1965년 국가 등록법 제정 이후로 개별적인 식별 번호가 국민에게 부여되고 있다. 국민 식별 번호를 활용한 인증 시스템인 Singpass가 2003년부터 도입되었으며, 이후 2018년에는 휴대용 앱인 Singpass Mobile이 제공되어 행정 및 민간 분야에서 디지털 본인 인증에 널리 사용되고 있다.

#### 2.1.2. 트러스트 프레임워크 개발 상황: National Digital Identity (NDI) Stack

디지털 ID 활용에 관한 국가 지침은 Singpass, My Info의 활용과 API를 통한 연결이 전제되어 있는 개념으로, 법적인 의무나 인증 체계는 존재하지 않으며, 정부 주도 영역(Singpass, My Info)과 민간 업체와의 협력을 통해 서비스 및 응용 분야의 체계가 제시되고 있다.

#### 2.1.3. 유스케이스

sgID의 개발 및 MyInfo의 개선 등에서 개별적인 식별 번호에 대한 의존을 약화시

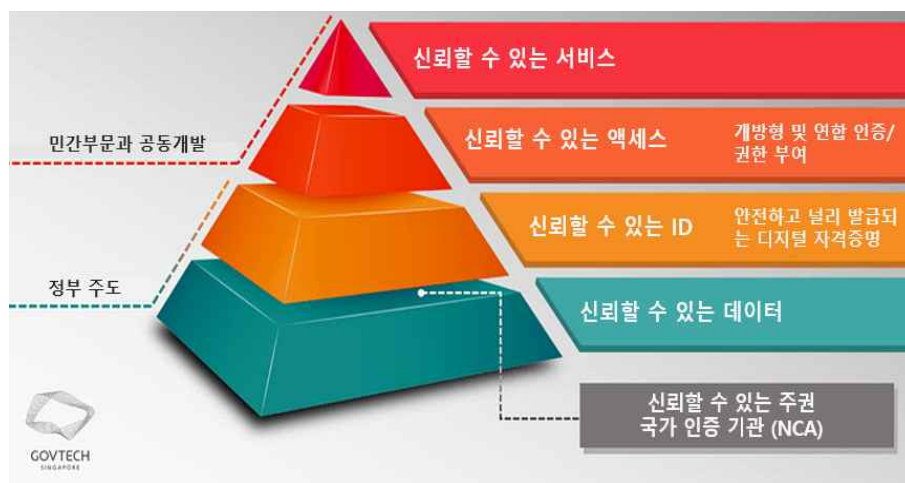
키고 분산형 모델을 고려하고 있다. 현재까지 개발된 유스케이스는 없다.

#### 2.1.4. 정책 방향

통일된 식별 체계를 활용하며, 이를 기반으로 정부가 주도하여 디지털 ID 서비스를 제공하고 있다. 프레임워크나 법률을 통해 세부 사항의 틀이나 요건을 정하는 것은 없으며, 디지털 ID 활용에 관한 국가 지침을 레이어 구조로 개념화하는데 그쳐 있다. 기존의 정부 제공 디지털 ID 서비스의 개선을 추구하면서 SSI/DID와 관련된 접근을 취하고 있다.

### 2.2. NDI Stack 피라미드

NDI Stack은 다음 그림과 같이 크게 4가지의 구성요소로 구분할 수 있다.



(그림 20) NDI Stack 피라미드

- o 신뢰할 수 있는 서비스
  - 공공기관 및 민간 부문 기업이 쉽게 플랫폼을 자체 서비스에 탑재할 수 있도록 API를 제공
- o 신뢰할 수 있는 액세스
  - SingPassMobile, 얼굴인증서비스 등 인증은 정부소유 인증모드로 이루어짐
  - 앱이나 사이트 내에서 자신의 ID를 확인할 수 있도록 연합 모델로 확장할 계획
- o 신뢰할 수 있는 ID
  - 출생시 모든 시민에게 발급되는 물리적 신분증과 생체인식을 포함
  - 중앙집중식 모델에서 작동하지만 다른 국가와의 상호운용성을 위해 분산형 배포 모델을 탐색 중

o 신뢰할 수 있는 데이터

- 다양한 정부기관의 데이터를 통합하는 MyInfo라는 데이터 플랫폼 출시
- MyInfo는 사용자 동의를 기반으로 사용자가 정부 또는 민간 부문 서비스와 거래 할 때 마다 반복적으로 제공할 필요가 없도록 보장

싱가포르의 NDI Stack에서 신뢰할 수 있는 서비스와 신뢰할 수 있는 액세스는 민간부문과 공공개발로 이루어지며, 신뢰할 수 있는 ID와 신뢰할 수 있는 데이터는 신뢰할 수 있는 주권국가 인증기관(NCA)를 통해 정부주도로 이루어진다.

### 3. 호주, Trusted Digital identity Framework(TDIF)

#### 3.1. 디지털 ID 정책의 방향

##### 3.1.1. 공통식별번호, 디지털 ID

과거에는 국민 ID 카드를 실현하기 위한 제안이 있었지만 모두 비판을 받아 실패했으며, Health Care 식별자나 Tax File Number 등 용도에 따라 여러 식별 번호를 사용하고 있다. 정부의 온라인 서비스에 액세스할 때 안전한 인증을 수행하기 위한 노력으로 디지털 ID 시스템을 촉진하고, 그를 지원하는 Trust Framework로 TDIF를 마련하고 있다.

##### 3.1.2. 트러스트 프레임워크 개발 상황

o Trusted Digital Identity Framework(TDIF)

- 호주 정부는 “디지털 ID 시스템” 내의 제공자와 서비스에 대한 엄격한 규칙과 표준을 규정

o Trust ID Framework

- 호주 민간 기업이 제공하는 디지털 ID 솔루션의 신뢰성과 상호 운용성을 높이기 위해 조직은 제품이나 서비스의 설계와 구축에서 준수해야 할 일련의 규칙과 지침을 규정

##### 3.1.3. 유스케이스

NSW 주에서의 디지털 ID에 대한 노력 중에서, 자기 주권형/분산형 ID에 관한 논의와 계획이 진행되고 있다. 현재까지 개발된 유스케이스는 2건으로 교육, 금융, 보험,

부동산 등 4개 분야에서 컨셉 단계 0건, PoC 단계 1건, 실제운영 1건으로 민간 기업에서 PoC와 실제운영 서비스 사례가 있다.

### 3.2. 정책 방향

통일된 식별번호는 검토되었지만 실행되지 않았으며, 목적에 맞는 식별번호를 사용하고 있다. 정부 주도의 디지털 ID 시스템을 위한 프레임워크인 TDIF와, 민간 주도로 정부와의 디지털 ID에 상호 운용성을 부여하는 노력이 병행되고 있다. 주정부 디지털 ID 관련 노력 중 SSI/DID로 추정되는 논의가 진행되고 있으며, 민간 기업에서 SSI/DID에 관한 PoC, 서비스 사례가 관찰된다.

## 4. 뉴질랜드, Digital Identity Trust Framework, Identity Management Standard

### 4.1. 디지털 ID 정책의 방향

#### 4.1.1. 공통식별번호, 디지털 ID

IRD(Individual Taxpayer's Identification Number) 번호, NHI(National Health Insurance) 번호, NSN(National Student Number) 등은 각각 세금, 의료, 교육 등의 목적에 따라 사용되는 여러 식별 번호이다. Digital Identity Trust Framework는 디지털 ID 서비스의 법적인 프레임워크를 규정하고, 디지털 ID 시스템을 위한 생태계로서 각 이해 관계자들을 보여준다.

#### 4.1.2. 트러스트 프레임워크 개발 상황

##### o Digital Identity Trust Framework

- 개인과 조직 간 거래를 위한 디지털 ID 서비스의 법적 프레임워크를 규정
- 신뢰할 수 있는 디지털 ID 서비스 사업자를 “TF 프로바이더”로 정의하고 등록하는 등의 제도를 마련

##### o Identity Management Standard

- 내무부에서 제정한 뉴질랜드의 ID 관리 표준은 각 보증 레벨과 그를 결정하는 식별 위험 평가에 따라 구성

#### 4.1.3. 유스케이스

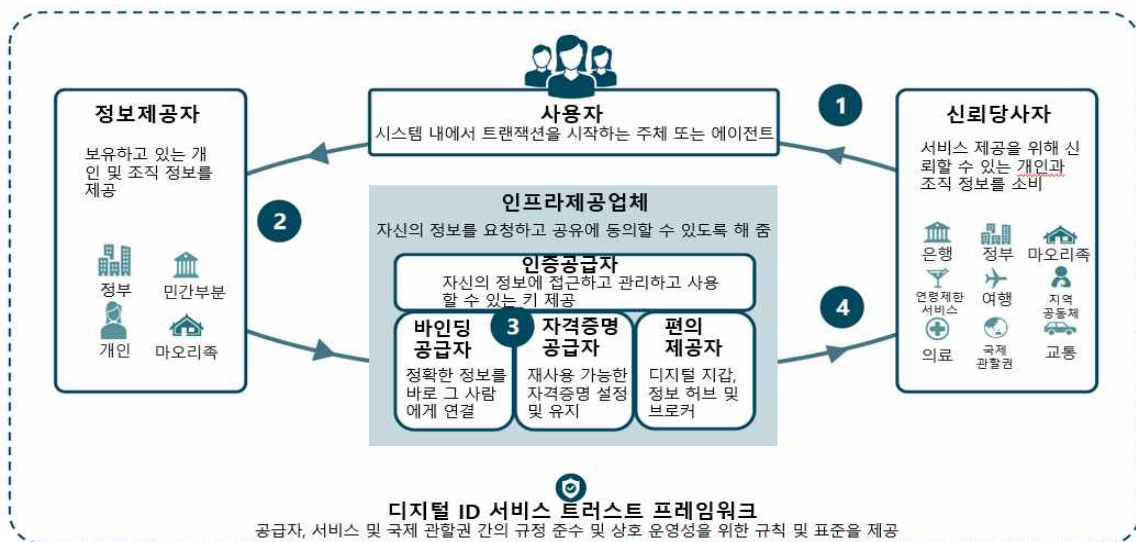
뉴질랜드 보건부는 2021년 코로나 백신 패스의 프로바이더로 오클랜드 IT 기업인 MATTR을 선정했다. MATTR 백신 패스는 DIF, ODF, W3C, IETF 등의 주요 국제 표준화 단체의 DID, VC 관련 규격을 지원하고 있다. 현재까지 개발된 유스케이스는 1건으로 의료분야에서 컨셉 단계 0건, PoC 단계 0건, 실제운영 1건으로 디지털 백신 패스에 분산형 ID를 채택한 유스케이스가 있다.

#### 4.1.4. 정책 방향

다른 목적에 대한 대체 식별 체계를 활용하며, 디지털 신분증에 대한 법적 틀을 마련하고 있다. 또한 정부는 신분 관리 표준을 수립하는 데 주도적인 역할을 하고 있다. SSI/DID와 관련된 지원 및 노력의 일환으로, 정부가 디지털 백신 패스에 분산형 신분증을 선택하는 것이 강조되고 있다.

#### 4.2. 디지털 ID 시스템(안)

다음 그림은 뉴질랜드의 디지털 ID 확인 시스템(안)을 설명하고 있는 다이어그램이다. 일반적인 거래 단계의 1에서 4까지 설명하고 있고, 참가자인 사용자, 신뢰파트너, 정보 공급자 및 인프라 공급자 간의 관계를 보여준다. 뉴질랜드의 디지털 ID 시스템은 포괄적인 디지털 ID 서비스 트러스트 프레임워크라 할 수 있다.



(그림 21) 뉴질랜드의 디지털 ID 시스템(안)

## 5. 인도, India Stack

### 5.1. 디지털 ID 정책의 방향

#### 5.1.1. 공통식별번호, 디지털 ID

2010년부터 얼굴 사진, 지문, 홍채, 이름, 주소 등의 등록과 12자리 식별 번호(Aadhaar 번호)를 부여하여 국민 신분증 기반인 Aadhaar를 구축하고 있다. Aadhaar를 기반으로 행정 기관과 민간 기업의 시스템에 Aadhaar를 연결하기 위한 오픈 API 집합을 포함한 국민 신분증 기반인 India Stack이 널리 활용되고 있다.

#### 5.1.2. 트러스트 프레임워크 개발 상황: India Stack

디지털 ID 활용에 관한 국가 지침은 Aadhaar의 활용과 API를 통한 연결을 전제로 개념화되었다. 이에 법적 강제력이나 인증 제도는 존재하지 않으며, Aadhaar를 기반으로 API를 통해 민간 업체 및 행정 서비스와의 연결을 통해 국민의 금융 포용을 추구하고 있다. Aadhaar는 OIX의 Trust Frameworks for Smart Digital ID에서 참조되고 있다.

#### 5.1.3. 유스케이스

Aadhaar 2.0에서는 블록체인 기술을 활용하여 분산형 수준의 솔루션을 구축하고, 선택적으로 정보를 제공하기 위한 지식증명 검토 등이 진행될 예정이다. 현재까지 개발된 유스케이스는 없다.

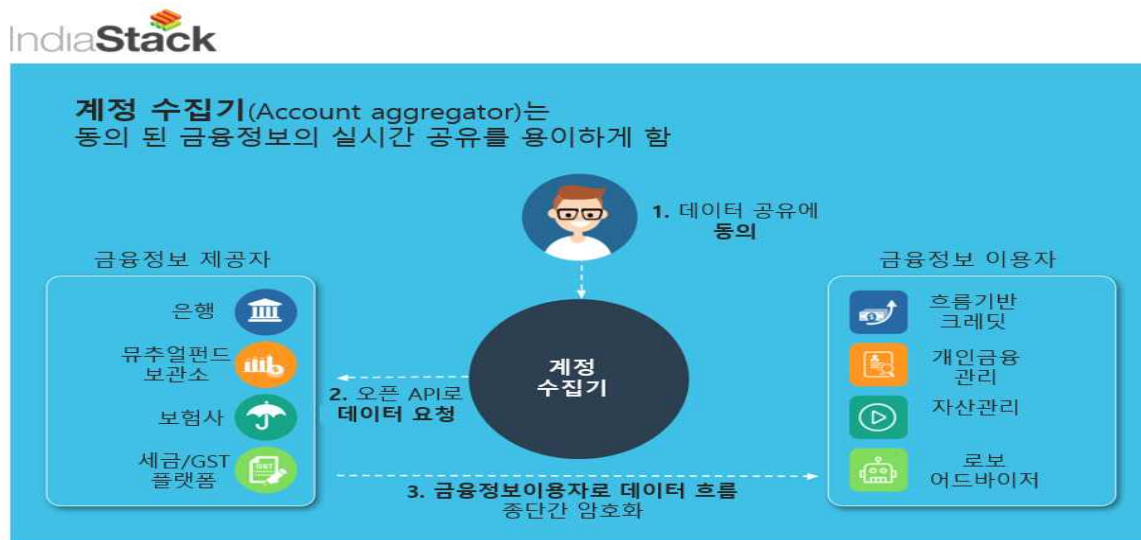
### 5.2. 정책 방향

통일된 식별 체계를 활용하여 정부가 주도하는 디지털 ID 서비스를 제공하고 있다. 프레임워크나 법률을 통해 세부 사항의 틀이나 요건을 정하는 것은 없으며, 디지털 ID 활용에 관한 국가 지침을 레이어 구조로 개념화하는 데 그치고 있다. 기존의 정부 제공 디지털 ID 서비스의 개선을 추구하면서 SSI/DID와 관련된 접근을 취하고 있다.

### 5.3. 계정수집기(Account Aggregator) 프레임워크

계정 수집기 프레임워크는 금융제품 구축을 방해하는 사용자 데이터 검색 및 공유의 시간과 비용을 더 이상 걱정하지 않아도 되는 인도의 새로운 데이터 민주주의를

위한 촉매제 역할을 한다. 소비자는 하나의 장소에서 모든 동의 계약을 승인, 관리, 철회할 수 있으며, 동시에 기관은 그들의 데이터 요청을 세분화된 수준에서 명확하게 정의할 수 있다. 개인과 기업은 권한없이 자신에 대한 모든 데이터를 검증 가능한 방식으로 증명할 수 있다.



(그림 22) Account Aggregator Framework

## 6. 한국

### 6.1. 모바일 신분증: 공무원증, 운전면허증

모바일 신분증은 개인 스마트폰에 안전하게 저장하여 편리하게 사용할 수 있는 신분증이다. 자기 정보를 관리할 수 있고 신원증명을 위해 필요한 정보만 선택적으로 제공할 수 있으므로 자기정보 결정권을 강화할 수 있다.

또한 안전한 보관 및 신원정보의 진위여부를 확인하기 위해 블록체인 기반 분산 ID를 사용하고 블록체인, 비대칭 암호화(PKI) 등 다양한 보안기술을 적용하여 안정성을 확보하였다. 모바일 신분증은 신원 및 자격 검증, 은행 고객 실명 확인, 렌터카 대여 등 다양한 영역에서 활용될 수 있다.

자기 정보의 결정권 강화, 안전한 신원정보 보관 및 검증, 거래정보의 보안성 강화를 기대할 수 있지만, 중앙화 플랫폼으로 완전한 개인정보 주권 보장에는 한계가 있고 개인 속성값에 대한 범위 한계를 가지고 있으며 기존 인증서 활용과의 차별성이 모호할 수 있는 한계점 또한 가지고 있다.





## 6.2. 금융분야 공공마이데이터

금융분야 공공마이데이터는 정보주체인 국민의 요구에 따라 행정 및 공공기관이 보유한 본인에 대한 행정정보를 본인 또는 제3자에게 제공하는 서비스이다. 국민이 행정 및 공공기관이나 금융 기관 등의 서비스를 신청하고 접수하는 경우 필요한 구비서류 정보를 한번에 묶어서 손쉽게 제출할 수 있다.

또한 공공 및 행정기관에서 보유중인 행정정보를 정보주체인 본인 또는 본인이 지정한 제3자에게 전송을 요구할 수 있는 데이터이다. 신용정보원은 금융분야에 활용되는 공공정보를 본인이 적극적으로 관리하고 통제할 수 있는 마이데이터 환경을 조성하고 있다.



(그림 24) 공공마이데이터 유통 체계

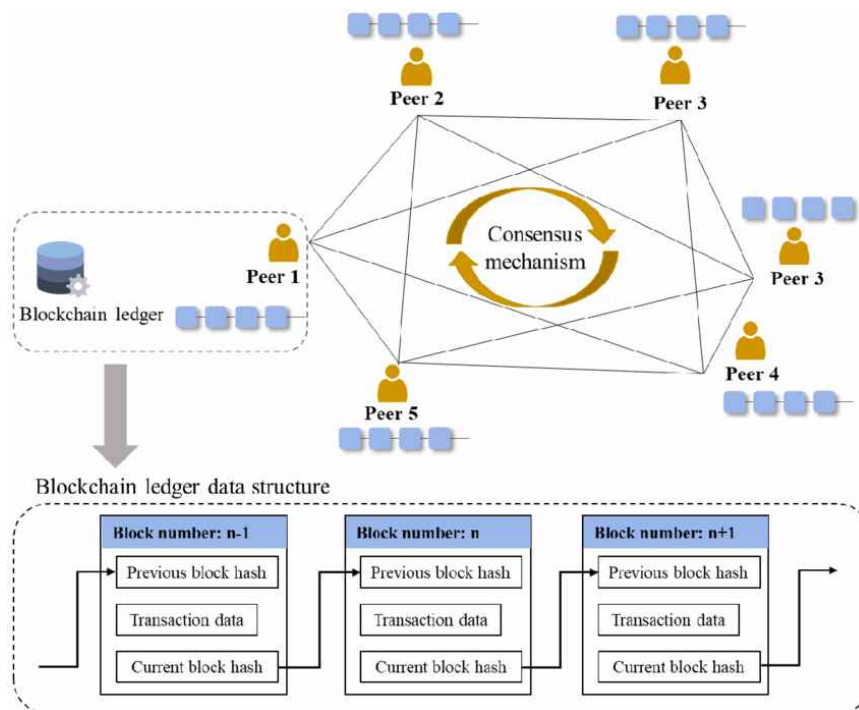
금융분야 공공마이데이터는 정보 주체의 자기정보 결정권을 보장하여 데이터의 주권을 강화시키고 행정 서비스의 신청과정, 구비 서류 제출을 간소화 시킬 수 있는 기대 효과가 있는 반면 중앙화 플랫폼으로 완전한 개인 정보 주권 보장이 어렵고 생태계 참여기업 증가시 개인정보 유출의 위험성이 잔존하며 정보주체의 실질적인 통제권 보장에는 한계가 있는 문제점 또한 존재한다.

## 제 3 장 Trusted Web 기반 기술

### 제 1 절 블록체인(Blockchain)

#### 1. 개요

블록체인(Blockchain)은 탈중앙화된 분산 데이터베이스 기술로, 여러 참여자 간의 신뢰에 기반한 분산원장 기술을 바탕으로 탈중앙화된 데이터베이스 시스템을 구축해 데이터에 대한 보안성, 투명성 및 무결성을 제공하는 시스템이다. 블록체인은 분산 원장 기술로서 데이터를 블록이라 불리는 연속적인 체인에 연결하여 저장하며, 이 블록들은 모든 참여자들에게 복제되어 저장된다. 블록체인 기술은 계속해서 발전하고 있으며 초기에는 암호화폐의 거래 기록을 관리하는 데 사용되었지만, 현재는 금융뿐만 아니라 다양한 산업 분야에서 활용되고 있다. 특히, 기업들은 블록체인을 비즈니스 프로세스의 효율성 향상과 안전한 데이터 관리에 활용하고 있다.



(그림 25) 블록체인 프레임워크

## 2. 블록체인 프로세스 및 구성 요소

### 2.1. 블록체인 프로세스

블록체인은 데이터베이스를 여러 참여자에게 분산하여 저장하고, 각 참여자는 전체 데이터베이스의 사본을 가지며, 변경이 있을 때마다 동기화되어 신뢰성과 안전성을 높인다. 블록체인 기술의 운영 플로우와 아키텍처는 여러 단계로 이루어져 있다.

[표 4] 블록체인 프로세스 및 내용

프로세스	내용
거래 생성 (Transaction Creation)	<ul style="list-style-type: none"> <li>- 사용자나 시스템이 새로운 거래를 생성</li> <li>- 이 거래에는 수신자, 송신자, 거래 금액 등의 정보 포함</li> </ul>
거래 검증 (Transaction Validation)	<ul style="list-style-type: none"> <li>- 생성된 거래는 블록체인 네트워크의 노드들에 의해 검증</li> <li>- 각 노드는 거래의 유효성을 확인하고, 송신자가 거래를 전송할 자격이 있는지 확인</li> </ul>
거래 브로드캐스팅 (Transaction Broadcasting)	<ul style="list-style-type: none"> <li>- 검증된 거래는 전체 네트워크에 브로드캐스트</li> <li>- 다른 노드들이 해당 거래를 수신하고 블록에 추가될 수 있도록 준비</li> </ul>
트랜잭션 풀 (Transaction Pool)	<ul style="list-style-type: none"> <li>- 브로드캐스트된 거래는 일시적으로 트랜잭션 풀에 저장</li> <li>- 풀은 아직 블록에 추가되지 않은 거래들을 저장</li> </ul>
블록 생성 (Block Creation)	<ul style="list-style-type: none"> <li>- 블록은 일정한 시간 간격 또는 일정 거래 수에 도달할 때마다 생성</li> <li>- 블록에는 트랜잭션들의 모음을 저장</li> </ul>
작업 증명 (Proof of Work)	<ul style="list-style-type: none"> <li>- 블록 생성 과정에서는 작업 증명이나 다른 합의 알고리즘을 사용하여 해당 블록이 네트워크에서 유효한 것을 증명</li> </ul>
블록 체인에 추가 (Adding to the Blockchain)	<ul style="list-style-type: none"> <li>- 유효성이 검증된 블록은 네트워크의 모든 노드에게 전파</li> <li>- 각 노드는 이 블록을 자신의 복사본에 추가</li> <li>- 이 과정을 통해 체인에 새로운 블록이 추가</li> </ul>
분산 원장 업데이트 (Updating the Distributed Ledger)	<ul style="list-style-type: none"> <li>- 새로운 블록이 추가되면 해당 블록에 포함된 거래 정보를 포함한 분산 원장이 모든 노드에 업데이트</li> </ul>
보상 및 트랜잭션 확정 (Rewarding and Transaction Finalization)	<ul style="list-style-type: none"> <li>- 작업 증명을 통해 블록을 생성한 노드는 새로운 코인을 보상받고 트랜잭션은 확정 및 완료</li> </ul>

## 2.2. 블록체인 구성요소

### 2.2.1. 분산 원장(Distributed Ledger)

분산 원장(Distributed Ledger)은 블록체인의 주요 구성 요소 중 하나로, 모든 참여자가 네트워크에 동일한 복제본을 가지고 있는 데이터베이스를 의미한다. 원장은 분산화되어 유지되고 중앙 관리자 없이 여러 참여자 간에 동기화되고 공유된다.

[표 5] 분산원장의 특징

특징	내용
분산화 (Decentralization)	분산 원장은 중앙화된 서버없이 여러 참여자에 의해 운영되므로 중앙 관리자나 중앙화된 통제가 없다.
신뢰성과 안전성 (Reliability and Security)	분산 원장은 각 노드에 복제되는 데이터로 구성되어 있으며, 이는 단일 지점의 고장이나 공격에 대한 내성을 제공하며 안전성을 높인다.
투명성 (Transparency)	모든 참여자는 동일한 복제본을 가지고 있어 데이터 변경 사항이 투명하게 나타나며, 거래의 실시간 추적이 가능하다.
불변성 (Immutability)	한 번 기록된 데이터는 변경이 어렵다. 블록체인에서는 이전 블록의 해시 값을 현재 블록에 사용하여 데이터의 불변성을 보장한다.

분산원장은 거래정보를 저장하고 관리하기 위해 거래, 블록, 합의 알고리즘 등으로 구성된다.

[표 6] 분산원장 구성요소

구성요소	내용
거래 (Transaction)	분산 원장에 저장되는 기본 데이터 단위는 거래입니다. 이는 블록에 포함되어 원장에 추가된다.
블록 (Block)	거래의 묶음은 블록이라 불리며, 각 블록은 이전 블록의 해시 값을 가지고 있어 체인처럼 연결되어 있다.
합의 알고리즘 (Consensus Algorithm)	네트워크 참여자 간에 합의를 도출하기 위한 알고리즘으로, 분산 원장을 유지하고 블록 추가 과정에서 사용된다.
분산 노드 (Distributed Nodes)	원장의 복제본을 유지하는 각 참여자는 분산 노드로서 역할을 합니다. 각 노드는 원장의 일관성을 유지하기 위해 네트워크와 상호 작용한다.
스마트 계약 (Smart Contracts)	프로그래밍 가능한 스마트 계약은 분산 원장에 포함되어 실행됩니다. 조건이 충족되면 자동으로 실행되는 프로그램 가능한 계약이다.

### 2.2.2. 블록(Block)

블록(Block)은 블록체인에서 기본적인 데이터 단위로, 여러 거래의 집합이나 다른 유형의 정보를 묶어서 저장하는 단위다. 각 블록은 이전 블록과 연결되어 체인을 형성하며, 이 체인은 블록의 해시(Hash)를 사용하여 무결성을 유지한다.

[표 7] 블락(Block) 구성요소

구성요소	내용
블록 헤더 (Block Header)	<ul style="list-style-type: none"> <li>- 버전(Version): 블록의 규칙과 기능을 정하는 프로토콜 버전</li> <li>- 이전 블록 해시(Previous Block Hash): 현재 블록 앞에 있는 이전 블록의 해시 값. 이전 블록과의 연결을 형성함으로써 체인을 구성</li> <li>- 머클 루트(Merkle Root): 트랜잭션들의 Merkle Tree(머클 트리)에서 얻은 루트 해시 값. 블록에 포함된 모든 트랜잭션의 무결성을 검증하는 데 사용</li> <li>- 타임스탬프(Timestamp): 블록이 생성된 시각</li> <li>- 난이도 목표(Bits): 블록을 생성하는 데 필요한 작업 증명(Proof of Work)의 난이도를 결정하는 값.</li> </ul>
트랜잭션 (Transaction)	<ul style="list-style-type: none"> <li>- 블록에 포함된 실제 데이터(거래 정보)</li> <li>- 여러 개의 트랜잭션을 하나의 블록에 묶어서 저장</li> </ul>
블록 해시 (Block Hash)	<ul style="list-style-type: none"> <li>- 블록 헤더와 포함된 트랜잭션 데이터를 해싱한 값</li> <li>- 블록의 식별자로 사용, 한 번 생성되면 수정 불가</li> </ul>
Nonce (논스)	<ul style="list-style-type: none"> <li>- 난이도 목표를 달성하기 위해 블록을 생성하는 과정에서 시도한 횟수를 나타내는 숫자</li> <li>- 올바른 논스 값을 찾는 것이 작업 증명의 핵심</li> </ul>
거래 데이터 (Transaction Data)	<ul style="list-style-type: none"> <li>- 블록에 포함된 모든 트랜잭션의 내용 포함</li> <li>- 거래의 송신자, 수신자, 금액 등과 같은 세부 정보 포함</li> </ul>
머클 트리 (Merkle Tree)	<ul style="list-style-type: none"> <li>- 블록에 포함된 여러 트랜잭션을 계층 구조로 구성한 트리</li> <li>- 머클 트리를 통해 트랜잭션의 일부만을 검증할 수 있고, 무결성을 효과적으로 확인 가능</li> </ul>

### 2.2.3. 스마트 컨트랙트 (Smart Contracts)

스마트 컨트랙트(Smart Contracts)는 블록체인 기술의 주요 구성 요소 중 하나로, 프로그래밍 가능한 계약으로서 코드로 작성되어 블록체인 네트워크에서 실행될 수 있는 자동화 계약이다. 스마트 컨트랙트는 특정 조건이 충족되면 코드에 정의된 작업을 수행하여, 기존 계약 및 거래의 자동화와 효율성을 제공하며, 특히 블록체인의 투명성, 보안성, 분산화된 특성을 활용하여 중앙 중재자 없이 안전하고 효율적으로 신뢰성 있고 자동화된 거래 및 계약을 가능하게 한다. 스마트 컨트랙트의 주요 특징은 아래와 같다.

- o 자동화된 실행 : 스마트 컨트랙트는 코드로 작성되어 중간에 사람의 개입없이 특정 조건이 충족되면 자동으로 실행된다.
- o 프로그래밍 가능성 : 스마트 컨트랙트는 프로그래밍 언어로 작성되며, 여러 언어에서 지원되는데 일반적으로는 Solidity, Vyper 등의 언어를 사용한다.
- o 불변성과 신뢰성 : 스마트 컨트랙트는 한 번 배포되면 변경이 어려우며 이는 블록체인의 불변성을 활용하여 신뢰성 있는 계약을 보장한다.
- o 분산 원장과 연동 : 스마트 컨트랙트는 분산 원장에 배포되어 각 참여자에게 복제되며, 이를 통해 모든 참여자가 동일한 계약 상태를 확인할 수 있다.
- o 조건부 실행 : 특정 조건이 충족되어야만 스마트 컨트랙트가 실행된다. 거래의 성사, 특정 시간 경과, 외부 이벤트 등에 따라 발생할 수 있다.
- o 비중재 및 중간자 제거 : 스마트 컨트랙트는 코드에 따라 자동으로 실행되므로 중재자나 중간자의 개입이 없이 거래를 진행할 수 있다.
- o 비용 절감과 효율성 : 중간자나 서류 작업 없이 자동으로 실행되므로 거래 비용을 절감하고, 빠르고 효율적인 거래 처리가 가능하다.

[표 8] 스마트 컨트랙트 구성요소

구성요소	내용
코드 (Code)	<ul style="list-style-type: none"> <li>- 스마트 컨트랙트는 프로그래밍 언어 코드로 작성</li> <li>- Ethereum의 경우, Solidity가 주로 사용됨</li> </ul>
상태 변수 (State Variables)	<ul style="list-style-type: none"> <li>- 스마트 컨트랙트는 상태 변수를 가질 수 있음</li> <li>- 컨트랙트의 현재 상태를 나타내며, 상태 변수의 값은 블록 체인에 저장되어 계속 유지됨</li> </ul>
함수 (Functions)	<ul style="list-style-type: none"> <li>- 스마트 컨트랙트에는 여러 함수가 정의됨</li> <li>- 함수들은 컨트랙트의 상태를 변경, 조회할 수 있으며, 네트워크 상의 특정 이벤트를 트리거할 수 있음</li> </ul>
이벤트 (Events)	<ul style="list-style-type: none"> <li>- 특정 상황 발생 시 알림을 보내는 이벤트 정의 가능</li> <li>- 이벤트는 블록체인에 기록되어 외부에서 감지</li> </ul>
모ডি파이어 (Modifiers):	<ul style="list-style-type: none"> <li>- 모ডি파이어는 함수의 동작을 수정하는데 사용</li> <li>- 예를 들어, 특정 권한이 있는지 확인하거나 특정 조건이 충족되었는지를 확인하는 데 사용 가능</li> </ul>
지불 (Payments)	<ul style="list-style-type: none"> <li>- 스마트 컨트랙트는 이더리움 같은 암호화폐 처리 가능</li> <li>- 함수의 실행 결과로 암호화폐를 송금하거나, 스마트 컨트랙트에 예치된 자금을 관리</li> </ul>
가스 (Gas)	<ul style="list-style-type: none"> <li>- 스마트 컨트랙트의 실행은 블록체인 네트워크에서 가스(Gas)라는 단위로 측정</li> <li>- 가스는 실행 비용을 나타내며, 컨트랙트를 실행하기 위해 소비되는 리소스를 의미</li> </ul>
배포 (Deployment)	<ul style="list-style-type: none"> <li>- 스마트 컨트랙트는 블록체인 네트워크에 배포</li> <li>- 배포는 새 컨트랙트를 블록체인에 추가하는 과정</li> <li>- 배포된 스마트 컨트랙트는 블록체인에서 수정 불가</li> </ul>

스마트 계약(Smart Contract)은 블록체인에서 실행되는 자동 계약으로, 조건이 충족되면 코드에 정의된 작업을 자동으로 실행하는 프로그램이다. 스마트 계약이 동작하는 과정은 아래와 같다.

#### ① 계약 생성

- 스마트 계약 작성 : 스마트 계약은 특정 블록체인 플랫폼에서 사용할 프로그래밍 언어로 작성된다. 특정 조건을 만족하면 실행할 작업에 대한 로직을 포함한다.
- 계약 배포 : 작성된 스마트 계약이 블록체인 네트워크에 배포되고, 블록체인의 특정 주소에 연결되어 다른 사용자들이 상호 작용할 수 있게 된다.

#### ② 계약 호출

- 트리거 이벤트 발생 : 스마트 계약은 특정 조건이나 이벤트가 발생했을 때 실행된다. 이벤트는 외부에서 발생할 수도 있고, 블록체인 내에서 다른 계약의 실행 결과 등 다양한 형태로 발생할 수 있다.
- 계약 호출: 이벤트가 발생하면 해당 스마트 계약이 호출된다. 호출은 특정 함수 또는 메서드를 실행하는 것을 의미한다.

#### ③ 계약 실행

- 조건 확인: 스마트 계약은 실행 전에 특정 조건을 확인하는데 프로그래밍된 로직에 따라 다르게 수행되며, 주로 사용자의 특정 조건 충족 여부를 확인한다.
- 트랜잭션 생성: 조건이 충족되면 스마트 계약은 해당 트랜잭션을 생성한다. 이 트랜잭션은 블록체인에 기록되어야 하는 작업을 의미한다.
- 트랜잭션 서명: 트랜잭션을 실행하기 위해서는 해당 트랜잭션에 대한 서명이 필요하다. 서명은 계약을 호출한 주체의 개인 키로 생성한다.

#### ④ 계약 실행 및 결과 기록

- 트랜잭션 전파: 서명이 붙은 트랜잭션이 블록체인 네트워크에 전파된다. 네트워크에 참여하는 노드들에게 해당 트랜잭션이 처리되어야 함을 알리는 과정이다.
- 트랜잭션 검증: 네트워크 상의 다수의 노드가 해당 트랜잭션을 검증하고, 스마트 계약이 올바르게 실행되는지 확인한다.
- 블록 생성: 검증 완료된 트랜잭션은 새로운 블록으로 묶여 블록체인에 추가된다.
- 계약 결과 기록: 스마트 계약이 실행된 결과, 즉 계약에서 정의한 작업이 수행된 내용이 블록체인에 기록된다.



### ⑤ 결과 확인

- 트랜잭션 확인: 블록이 생성되고 네트워크에 분산되면, 스마트 계약 호출자 및 다른 사용자들은 블록체인을 통해 계약의 결과를 확인할 수 있다.
- 이벤트 발생 (옵션): 스마트 계약이 실행된 결과로 다시 새로운 이벤트가 발생할 수 있다. 다른 스마트 계약이나 응용 프로그램이 연쇄적으로 실행될 수 있다.

스마트 계약은 이러한 과정을 통해 자동화된 계약 실행 및 결과 기록을 제공하며, 블록체인의 탈중앙화된 특성을 활용하여 안전하게 이루어진다.

[표 9] 스마트 컨트랙트 동작 과정

구성요소	내용
1. 스마트 컨트랙트 개발	프로그래머가 특정 스마트 컨트랙트를 개발하고, 원하는 조건과 작업을 코드로 작성한다.
2. 블록체인 네트워크 배포	개발된 스마트 컨트랙트 코드는 블록체인 네트워크에 배포된다. 배포 시점에서 스마트 컨트랙트가 특정 주소에 연결된다.
3. 트리거 이벤트 발생	스마트 컨트랙트가 실행되어야 하는 조건이 충족되면 (예: 특정 거래가 발생하거나 시간이 경과) 스마트 컨트랙트가 실행될 이벤트가 발생한다.
4. 스마트 컨트랙트 실행	이벤트 발생에 따라 스마트 컨트랙트 코드가 실행되어 특정 작업이 수행된다.
5. 분산 원장 업데이트	스마트 컨트랙트가 실행되면 해당 거래와 결과는 블록에 추가되어 분산 원장이 업데이트된다.

#### 2.2.4. 분산 합의 알고리즘 (Distributed Consensus Algorithm)

분산 합의알고리즘(Distributed Consensus Algorithm)은 블록체인에서 여러 참여자 간에 동일한 거래 내용 및 상태를 동기화하고 합의하는 메커니즘을 제공하는 알고리즘이다. 다양한 참여자들이 분산된 환경에서 동일한 결정에 도달할 수 있도록 보장하여 블록체인의 일관성과 무결성을 유지하는데 사용된다. 분산 합의 알고리즘은 중앙화된 서버없이 분산된 환경에서 작동하므로, 네트워크 내에서 발생할 수 있는 여러 문제에 대비하여 설계된다. 각 참여자들의 의견 차이나 악의적인 행위에도 블록체인의 일관성과 무결성을 유지하기 위한 필수요소이며 다음의 특징을 가진다.

- o 비잔틴 장애 내성 (Byzantine Fault Tolerance, BFT) : 분산 합의 알고리즘은 참여자들 중 일부가 악의적인 행위를 할 수 있거나 장애 상태일 때에도 정상적

인 합의를 도출할 수 있어야 한다.

- o 분산 환경 고려 : 블록체인은 여러 참여자와 노드들 간에 분산된 환경에서 작동하므로 네트워크 지연, 패킷 손실 등과 같은 조건을 고려해야 한다.
- o 안정성과 확장성 : 합의 알고리즘은 시스템이 안정적으로 동작하면서도 높은 트랜잭션 처리량을 지원할 수 있어야 한다.
- o 다수 결정 (Majority Decision) : 대부분의 참여자들이 동의해야만 합의가 이루어지는 다수결 원칙이 적용된다.

이러한 분산 합의 알고리즘들은 블록체인의 핵심적인 원칙인 분산, 보안, 무결성을 지원하며, 각각의 알고리즘은 특정 상황이나 필요에 따라 선택해서 사용하게 된다. 알고리즘 선택은 특히 네트워크의 특성, 사용자의 목표, 보안 요구사항 등에 따라 달라지는데 다양한 분산 합의 알고리즘이 존재한다.

[표 10] 분산 합의 알고리즘의 종류

알고리즘	내용
Proof of Work (PoW)	컴퓨팅 파워를 사용하여 블록을 생성하는 방식으로, 네트워크 참여자 중 가장 먼저 문제를 해결한 노드가 새로운 블록을 생성할 권한을 갖는다.
Proof of Stake (PoS)	보유한 코인의 양에 비례하여 블록을 생성하는 방식으로, 코인을 보유한 비율이 높을수록 블록 생성에 우선한다.
Delegated Proof of Stake (DPoS)	PoS의 변형으로, 네트워크 참여자들이 대표자를 선택하여 그들에 의해 블록이 생성되는 방식이다.
Practical Byzantine Fault Tolerance (PBFT)	비잔틴 장애에 내성있는 BFT 알고리즘으로, 노드들 간에 투명한 통신을 통해 합의를 도출한다.
Raft	네트워크에서 리더 노드가 선출되어 합의를 도출하는 방식으로, PBFT와 유사한 목표를 가지고 있다.
HoneyBadgerBFT	비잔틴 장애에 내성있는 BFT 알고리즘 중 하나로, 노드 간의 비동기적 통신을 통해 합의를 형성한다.

블록체인은 탈중앙화된 분산 데이터베이스 기술로, 각 거래가 암호화되어 체인상에 영구적으로 기록된다. 블록체인의 주요 특징은 분산원장(Decentralized Ledger)과 불변성(Immutability)이다.

## 제 2 절 대체 불가능 토큰(NFT)

### 2.1. 개요

NFT는 비트코인, 이더리움 등의 암호화폐와 유사하게 블록체인 기술을 활용하여 위·변조가 불가능하게 저장되는 디지털 데이터 단위다. NFT는 블록체인 기술을 활용하여 토큰을 발행하고 해당 토큰 안에 특정 데이터를 저장함으로써 온라인 환경에서 해당 데이터에 대한 고유성을 확보하게 된다. NFT는 디지털콘텐츠에서 유일성을 확보하고 거래 투명성이 보장되므로 디지털 환경에서의 활용이 주목되고 있다. NFT는 각각이 고유한 식별자를 가지며, 이를 통해 각 토큰이 유일하게 식별된다. ERC-721은 이더리움 블록체인 상에서 고유한 토큰을 정의하는 표준을 제공한다. 블록체인에 기록된 정보는 변경이 어렵기 때문에 각 NFT는 중복되지 않고 유일하게 소유된다. 또한 블록체인은 불변성을 가지며, 한 번 기록된 정보는 변경이 어려우며 NFT의 소유권 변경이나 특정 속성의 업데이트는 블록체인 상에 기록되어 전체 네트워크에서 확인할 수 있다. NFT는 디지털 자산의 소유권을 투명하게 기록하고 거래할 수 있는 혁신적인 기술로, 블록체인과 암호화폐 생태계에 중요한 영향을 미치고 있다.

### 2.2. NFT 주요 구성요소

Non-Fungible Token(NFT)는 블록체인을 기반으로 하며, 스마트 컨트랙트, 토큰 표준, 지갑, 그리고 사용자 간의 거래 등으로 구성된다.

[표 11] NFT 주요 구성요소

구성요소	내용
스마트 컨트랙트	<ul style="list-style-type: none"> <li>- NFT의 핵심 기능은 스마트 컨트랙트에서 정의</li> <li>- NFT의 발행, 전송, 소유권 관리 등의 로직을 포함</li> </ul>
토큰 표준	<ul style="list-style-type: none"> <li>- 토큰 표준은 NFT의 동작 규칙을 정하는 인터페이스</li> <li>- ERC-721 및 ERC-1155와 같은 표준은 NFT의 유일성, 소유권 이전, 메타데이터 관리 등에 대한 규칙을 정의하여 상호 운용성을 증가</li> </ul>
Wallet	<ul style="list-style-type: none"> <li>- 사용자는 Wallet(지갑)을 통해 자신의 NFT를 관리하고 거래</li> <li>- 지갑은 사용자의 공개키와 개인키를 생성하고 보관하여 블록체인에 기록된 자산에 접근하며, NFT를 전송하거나 받을 수 있음</li> </ul>

## 2.2. NFT 토큰 ID 구조

고유한 식별자(Token ID)는 Non-Fungible Token(NFT)에서 각각의 토큰을 식별하는 데 사용되는 고유한 값이며, 일반적으로 숫자나 문자열로 표현된다. Token ID의 구조는 특정 토큰의 고유성을 나타내기 위해 디자인되며, 토큰 표준과 스마트 컨트랙트에서의 사용 방식에 따라 다양한 형태를 가질 수 있다. 대표적인 NFT 표준인 ERC-721과 ERC-1155를 예로 들어보면 아래와 같다.

### o ERC-721의 Token ID 구조

- ERC-721은 Ethereum에서 가장 일반적으로 사용되는 NFT 표준 중 하나
- 각 토큰은 256비트의 정수로 표현되는 고유한 Token ID를 보유
- 예) plaintextCopy code

Token ID: 123

특정 NFT의 Token ID는 123

### o ERC-1155의 Token ID 구조

- ERC-1155은 다중 자산을 하나의 계약으로 관리하는 NFT 표준
- 각 토큰의 고유성을 나타내기 위해 다양한 데이터 형식 사용 가능
- 일반적으로 정수, 바이트 배열, 또는 문자열로 표현
- 각 토큰은 256비트의 정수로 표현되는 고유한 Token ID를 보유
- 예) plaintextCopy code

Token ID: "0xabcdef123456"

"0xabcdef123456"는 12자리의 16진수로 나타낸 Token ID

## 2.3. NFT 동작 과정

토큰의 고유성을 나타내기 위해 Token ID 구조는 토큰 표준 및 스마트 컨트랙트에서의 사용 목적에 따라 달라질 수 있다. 일반적으로 숫자 또는 문자열로 표현되지만, 특정 표준이나 프로젝트에서는 추가적인 데이터나 암호화된 형태의 구조를 사용할 수도 있다. NFT의 Token ID는 해당 토큰의 고유한 식별자이며, 블록체인에서 소유권 및 거래 추적에 중요한 역할을 한다. NFT는 주로 블록체인에서 디지털 자산의 소유권을 나타내는 토큰으로 사용되며, 플로우는 주로 블록체인에서 디지털 자산의 소유권을 나타내고 전송하는 과정을 포함한다. NFT의 동작은 스마트 컨트랙트를 통해 이

루어지며, 사용자는 지갑을 사용하여 자신의 NFT를 관리하고 거래한다.

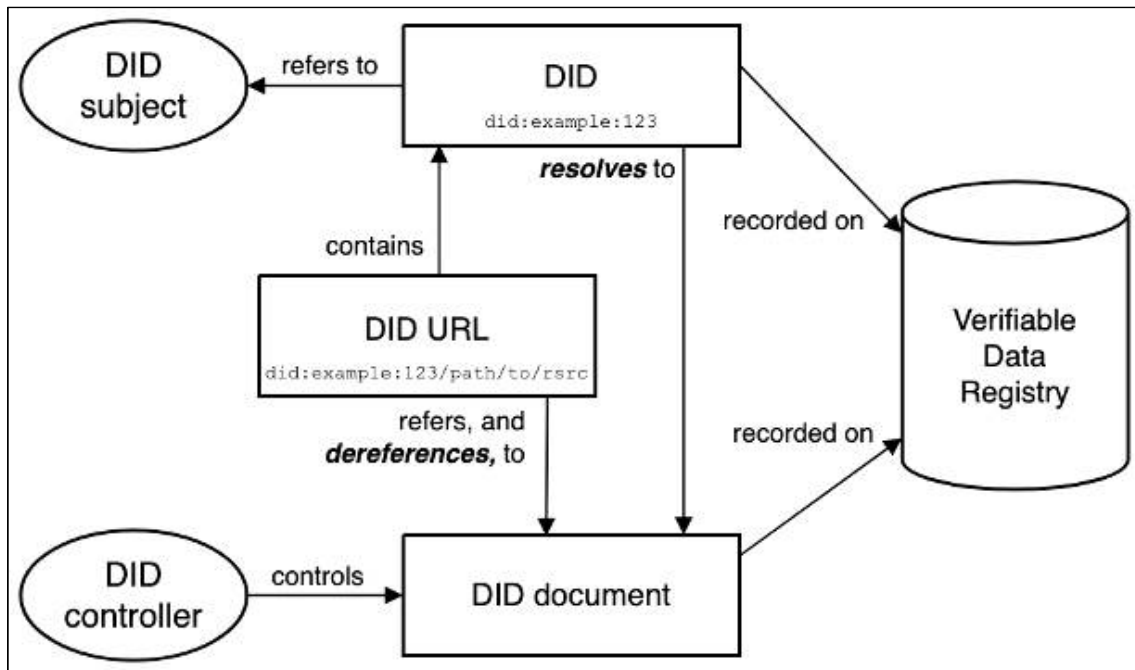
[표 12] NFT 동작 과정

프로세스	내용
1. 토큰 발행 (Minting)	<ul style="list-style-type: none"> <li>- 스마트 컨트랙트를 통해 NFT의 발행</li> <li>- 스마트 컨트랙트는 NFT를 새로 생성하고, 각 토큰에는 고유한 Token ID와 메타데이터 할당</li> </ul>
2. 거래	<ul style="list-style-type: none"> <li>- 사용자는 지갑을 사용해 NFT를 다른 사용자에게 전송 가능</li> <li>- 스마트 컨트랙트는 소유자의 변경을 처리하고, 블록체인 네트워크에 이를 기록</li> </ul>
3. 조회 및 메타데이터	<ul style="list-style-type: none"> <li>- 사용자는 지갑을 통해 소유한 NFT를 확인</li> <li>- 각 토큰의 메타데이터를 조회 가능</li> <li>- 메타데이터는 예술 작품의 설명, 속성, 이미지 등을 포함</li> </ul>
4. 이벤트 및 알림	<ul style="list-style-type: none"> <li>- NFT 상태변경이나 특정 이벤트 발생 시, 스마트 컨트랙트는 이벤트를 발생시키고 네트워크에 통보</li> <li>- 이벤트 알림을 통해 사용자 인터페이스나 외부 응용 프로그램에서 상태 변화를 실시간으로 감지 가능</li> </ul>
5. 시장 및 거래소	<ul style="list-style-type: none"> <li>- 다양한 NFT 시장과 거래소는 사용자들이 NFT를 거래하고 찾을 수 있는 플랫폼을 제공</li> <li>- 사용자는 플랫폼에서 NFT를 구매하거나 판매</li> </ul>
6. 소유자 확인 및 검증	<ul style="list-style-type: none"> <li>- 블록체인은 불변성과 투명성을 제공</li> <li>- 각 NFT의 소유권은 블록체인 상에서 확인 및 검증</li> <li>- 특정 NFT의 거래 이력 추적 가능</li> </ul>

## 제 3 절 분산 ID(Decentralized IDentity)

### 3.1. 개요

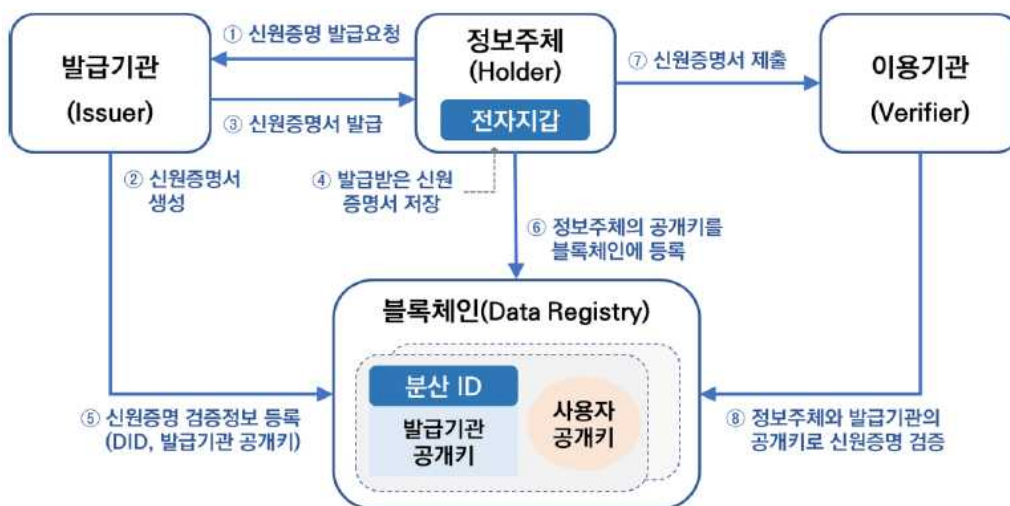
분산 ID(Decentralized IDentity, DID)는 분산된 데이터베이스 또는 블록체인 기술 기반으로 개인 또는 객체의 디지털 신원을 관리하는 방식을 말하며 사용자는 자체적으로 신원을 제어하고 보안성과 프라이버시를 강화한다. 분산 ID의 특징으로는 공개 키를 블록체인에 게시하는 분산형 PKI 방식을 적용한 ‘분산원장 기반 신원관리’, 명시적 동의 없이 서비스 제공자의 개인정보를 활용하는 것을 제한할 수 있는 ‘개인정보 보호 강화’, 사용자 기기에 저장된 자격증명(Credential)을 검증하여 신원을 확인하는 ‘개인 ID를 개인에 귀속’ 등이 있다.



(그림 26) DIDs 프레임워크

### 3.2. 분산 ID(DiDs, Decentralized Identifiers) 주요 구성요소

DiDs는 중앙 집중식이 아닌 식별자 시스템으로, 블록체인과 분산 원장 기술을 기반으로 하여 사용자 및 기기의 식별을 위한 개념이다. DiDs는 사용자가 자신의 식별자를 소유하고 관리할 수 있도록 하여 디지털 신원의 소유와 제어를 개선하는 것을 목표로 한다. 다음 그림은 분산 ID 관리의 구조 및 절차를 보여준다.



(그림 27) 분산 ID 관리 구조 및 발급/검증 절차

### 3.2.1. Verifiable Credentials(VCs)

Verifiable Credentials(VCs)는 분산 식별자(DIDs)와 함께 사용되는 디지털 인증서로, 신원 및 권한 정보를 안전하게 전달하고 검증하기 위한 표준화된 방법을 제공한다. Verifiable Credentials는 자체 서명을 포함하여 신뢰성을 보장하며, 다양한 컨텍스트에서 사용될 수 있다.

#### ① Verifiable Credentials의 구성 요소:

- Claim (주장) : Verifiable Credential에는 주장(claim)이 포함되어 있다. 주장은 특정 주체(Subject)에 대한 정보를 나타내며, 신원, 권한 또는 다른 속성에 대한 내용을 포함한다.
- Credential Subject (자격 증명 주체) : Credential Subject는 Verifiable Credential에 포함된 주장에 대한 주체를 나타낸다. 주체는 일반적으로 DID와 연결되어 해당 DID에 속한 개체를 식별한다.
- Issuer (발급자) : Issuer는 Verifiable Credential을 발급한 주체를 의미한다. Issuer는 DID를 통해 식별되며, Credential을 발급하는 권한을 가지고 있다.
- Issuance Date (발급일) : Verifiable Credential의 발급일은 Credential이 언제 발급되었는지를 나타낸다.
- Expiration Date (만료일) : Credential에는 유효 기간이 있어서 Credential이 언제까지 유효한지를 나타내는 만료일이 포함될 수 있다.
- Digital Signature (디지털 서명) : Verifiable Credential은 발급자에 의해 디지털 서명되어 있어야 한다. 이 서명은 Credential의 무결성을 보장하고 발급자를 신뢰할 수 있도록 한다.

### 3.2.2. DID Methods

DID Methods(분산 식별자 메소드)는 분산 식별자(DIDs)를 생성하고 관리하기 위한 특정한 방법 또는 규칙을 의미한다. 각 DID Method는 고유한 식별자를 생성하고 해당 식별자에 대한 정보를 관리하는 방식을 정의하며, 분산된 환경에서 신원을 관리하는 데 사용된다. 여러 DID Methods가 존재하며, 각각은 다른 블록체인, 분산 레지스트리, 또는 식별 체계를 기반으로 한다.

#### ① DID Methods 구성요소

- Method-Specific Identifier (메소드별 식별자) : 메소드별 식별자는 각 메소드에 특정한 형식을 가진 DID를 생성하기 위한 고유한 식별자이다. 이는 해당 메

소드에 따라 다양한 형식으로 존재할 수 있다.

- Method-Specific DID Document : 각 메소드는 DID Document의 구조를 정의하고, 해당 메소드에서 생성된 DID와 연결된 정보를 담고 있는 DID Document를 관리한다.
- Method-Specific Operations : 각 메소드는 DID를 생성하고 관리하기 위한 특정한 연산이나 프로토콜을 제공한다. 해당 메소드의 동작을 결정하는 중요한 요소이다.

## ② DID Method의 예시

- did:eth (Ethereum-based DID Method)
- 메소드 이름: eth
- Identifier Generation: Ethereum 주소를 기반으로 DID를 생성
- DID Document 구조 : Ethereum 주소, 공개키, 서비스 엔드포인트 등을 포함
- did:web (Web-based DID Method):
- 메소드 이름: web
- Identifier Generation: URL을 기반으로 DID를 생성
- DID Document 구조: 공개키, 서비스 엔드포인트 등을 포함

### 3.2.3. DID Documents

DID에 대한 정보를 포함하고 있는 DID Documents(분산 식별자 문서)는 해당 DID의 소유자가 공개키, 서비스 엔드포인트, 인증 방법 등과 같은 다양한 신원과 관련된 정보를 포함한다. DID Documents는 분산 식별 체계에서 디지털 신원을 정의하고 공유하는 데 필수적인 구성 요소이다.

#### ① DID Documents의 역할

- 디지털 신원 관리 : DID Documents는 DID 소유자가 자신의 디지털 신원을 관리하는 데 사용된다. 공개키 및 서비스 엔드포인트 정보를 통해 다른 사용자가 해당 신원을 신뢰할 수 있게 한다.
- 디지털 서명 및 검증 : authentication 섹션에서 정의된 인증방법을 사용하여 DID 소유자는 디지털 서명을 하고, 다른 사용자는 서명을 검증할 수 있다.
- 서비스 제공 : DID와 연관된 서비스 엔드포인트 정보를 제공한다. 다른 사용자는 DID 소유자와 상호 작용 또는 특정 서비스를 활용할 수 있다.
- DID 해석 : DID Resolver는 특정 DID를 해석하여 연결된 DID Document를 가



저온다. 이를 통해 DID의 정보를 조회할 수 있다.

[표 13] DID Documents 구성요소

구성 요소	내용
@context	<ul style="list-style-type: none"> <li>- @context는 JSON-LD 문서로 DID Document의 컨텍스트를 정의</li> <li>- DID Document 내의 정보 해석 방법을 제공</li> </ul>
id	<ul style="list-style-type: none"> <li>- id는 DID Document 자체의 고유한 식별자</li> <li>- 해당 문서의 URL이나 URI 제공</li> </ul>
publicKey	<ul style="list-style-type: none"> <li>- publicKey는 DID와 연결된 공개키 정보를 포함하는 배열이나 리스트로서 각 공개키 항목은 키의 유형(type), 값(value), 컨트롤러(controller) 등을 포함</li> </ul>
authentication	<ul style="list-style-type: none"> <li>- authentication은 DID와 연관된 인증 방법 표현</li> <li>- 이 방법을 통해 DID 소유자가 디지털 서명을 생성</li> </ul>
service	<ul style="list-style-type: none"> <li>- 각 서비스 항목은 서비스의 유형, 엔드포인트(endpoint), 수명주기(lifecycle) 등 서비스 엔드포인트 정보를 담고 있는 배열이나 리스트</li> </ul>
created 및 updated	<ul style="list-style-type: none"> <li>- created는 DID Document가 생성된 날짜</li> <li>- updated는 마지막으로 문서가 업데이트된 날짜</li> </ul>
proof (Optional)	<ul style="list-style-type: none"> <li>- proof는 DID Document의 디지털 서명을 포함할 수 있는 선택적인 요소</li> <li>- DID Document의 무결성 검증에 사용</li> </ul>

### 3.2.4. DID Authentication

DID Authentication은 사용자가 DID를 사용하여 시스템이나 서비스에 안전하게 로그인하고 인증하는 방법을 다룬다. DID를 사용한 안전한 인증은 중앙 집중형 인증 체계와는 다른 방식으로 작동한다.

#### ① DID Authentication의 핵심요소

- Public Key (공개키) : DID와 연결된 공개키는 DID 소유자가 자신의 신원을 증명하는 데 사용된다. 해당 공개키는 DID Document 내의 publicKey 섹션에 정의된다.
- Authentication Method (인증 방법) : DID Document는 authentication 섹션을 포함한다. 이 섹션에는 DID 소유자가 자신을 인증하기 위해 사용하는 인증 방법(공개키)이 정의된다.
- Digital Signature (디지털 서명) : DID 소유자는 자신의 신원을 증명하기 위해 특정한 인증 방법(공개키)을 사용하여 데이터에 디지털 서명을 생성한다. 서명은 해당 데이터가 소유자에 의해 생성되었음을 확인하는데 사용된다.
- Challenge-Response Mechanism (도전-응답 메커니즘) : 인증을 요청하는 도

전(challenge)이 오면 DID 소유자는 해당 도전에 대한 서명을 생성하여 응답(response) 한다. 누구나 도전에 대한 서명을 생성할 수 있는지 확인함으로써 공격자로부터의 보호를 강화한다.

## ② DID Authentication의 작동 방식

DID Authentication은 사용자가 자신의 디지털 신원을 증명할 수 있도록 하며, 공개키 및 디지털 서명을 활용하여 보안적으로 신뢰할 수 있는 방식으로 이루어진다. 이는 분산 식별 체계에서 중요한 요소로써 자주 발생하는 사용자의 로그인 및 인증 문제를 해결하기 위한 혁신적인 방법 중 하나이다.

[표 14] DID Authentication의 작동 방식

과정	내용
인증 요청	- 사용자나 시스템이 특정 DID에 대한 인증 요청
Challenge 전달	- 인증 서비스는 사용자에게 도전(Challenge)을 전달 - 도전(Challenge)은 무작위 또는 애플리케이션에서 생성된 랜덤한 값
DID 소유자의 응답	- DID 소유자는 DID Document에서 찾은 인증 방법(공개키)을 사용하여 도전에 대한 서명을 생성
서명 검증	- 인증 서비스는 DID 소유자의 응답과 해당 DID의 DID Document에서 찾은 공개키를 사용하여 서명의 유효성을 검증
인증 결과 전송	- 서명이 유효하면 사용자는 인증성공으로 판단 - 이 정보는 인증 서비스를 통해 전송

### 3.2.5. DID Resolver

DID Resolver(분산 식별자 해석기)는 특정 DID(분산 식별자)를 해석하고, 해당 DID에 연결된 DID Document를 검색하는 역할을 수행하는 도구 또는 서비스를 말한다. DID Resolver는 DID를 특정 환경에서 해석하여 신원 정보나 디지털 서명을 검증하는 데 사용된다.

#### ① DID Resolver의 주요 특징

- DID Resolution : DID Resolver는 DID를 해석하여 해당 DID에 연결된 DID Document를 가져온다. 이 과정은 DID를 사용하여 특정 주소나 식별자에 연결된 정보를 검색하는 것을 의미한다.

- DID Document 검색 : DID Resolver는 DID Document를 검색하고 가져오는 데 사용된다. DID Document에는 DID와 관련된 정보, 공개키, 서비스 엔드포인트, 컨트롤러 정보 등이 포함된다.
- Contextual Information 처리 : DID Resolver는 DID Document를 해석할 때 컨텍스트 정보를 사용하여 해당 문서의 의미를 이해한다. 주로 JSON-LD 형식의 컨텍스트를 활용한다.
- DID Method 별 처리 : DID Resolver는 다양한 DID Methods에 대해 특정 처리를 수행할 수 있다. 각 DID Method는 다른 방식으로 DID를 생성하고 관리하므로, Resolver는 이러한 차이점을 이해하고 처리할 수 있어야 한다.
- Caching 및 성능 최적화 : 일부 Resolver는 이전에 검색한 DID Document를 캐시하여 성능을 최적화할 수 있다. 동일한 DID에 대한 반복적인 검색에서 성능을 향상시킬 수 있다.

## ② DID Resolver의 작동 방식

- DID Resolver는 DID의 상호 운용성에 중요한 역할을 하며, Resolver의 구현은 DID Method 및 사용 사례에 따라 다양하게 이루어진다.

[표 15] DID Resolver의 작동 방식

과정	내용
DID 입력	- 사용자 또는 시스템이 특정 DID를 제공
DID Resolver 호출	- DID Resolver가 특정 DID에 대한 해석을 수행
DID Document 검색	- Resolver는 DID에 연결된 DID Document를 검색 - 블록체인, 분산 레지스트리, 또는 다른 저장소에서 정보를 가져오는 등의 다양한 방법으로 수행
DID Document 반환	- Resolver는 검색된 DID Document를 반환 - 이 문서에 DID와 관련된 정보, 공개키, 서비스 엔드포인트 등이 포함
결과 전달	- Resolver는 DID Document를 호출한 사용자 또는 시스템에 전달하여 해당 DID에 관한 정보를 제공

### 3.2.6. DID Controller

DID Controller(분산 식별자 컨트롤러)는 DID와 관련된 특정 DID Document의 권한을 가진 주체를 의미한다. DID Controller는 DID 소유자가 아닌 다른 주체가 특정

DID와 관련된 작업을 수행할 권한을 가지도록 허용하는 주체이며, 이러한 권한은 주로 공개키의 사용, DID Document의 업데이트, 서비스 엔드포인트의 등록과 같은 작업을 포함한다. 아래와 같은 특징을 지닌다.

① 권한 부여

- DID Controller는 DID Document 내에서 자신의 공개키를 통해 권한을 부여받고 다른 주체가 해당 DID에 대한 특정 작업을 수행할 수 있게 한다.

② 공개키 관리

- DID Controller의 공개키는 DID Document 내의 publicKey 섹션에 정의된다. 다른 사용자는 이 공개키를 사용하여 해당 DID Controller의 디지털 서명을 확인하고 권한을 검증할 수 있다.

③ DID Document 업데이트

- DID Controller는 해당 DID의 DID Document를 업데이트할 수 있는 권한을 가진다. DID 소유자는 이를 사용하여 신원 정보를 업데이트하거나 DID Document의 일부를 변경할 수 있다.

④ 서비스 엔드포인트 등록

- DID Controller는 DID Document에 서비스 엔드포인트를 등록하거나 업데이트하고, DID와 연결된 서비스에 대한 정보를 유지하고 업데이트할 수 있다.

⑤ DID Controller 예시

- DID Document 내의 publicKey 섹션에서 각 공개키 항목은 해당 공개키를 사용하여 DID Document를 서명한 컨트롤러를 나타낸다.

```
{
  "id": "did:example:123456",
  "publicKey": [
    {
      "id": "#keys-1",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:example:123456",
      "publicKeyBase58": "..."
    },
    // Additional public keys may be listed here
  ],
  // Other parts of the DID Document
}
```

- 위의 예시에서 “controller”: “did:example:123456”는 해당 공개키의 소유자, 즉 컨트롤러가 “did:example:123456”의 DID를 가진 주체임을 의미한다.
- DID Controller는 DID의 관리와 권한 위임을 통해 분산 식별 체계에서 신뢰성 있는 신원 관리를 지원한다. DID 소유자가 필요한 경우 다른 주체에게 일부 권한을 위임하거나 특정 작업을 수행하도록 하는 데 중요한 역할을 한다.

### 3.2.7. DID URL

DID URL(분산식별자 URL)은 특정 DID(Document Identifier)를 가리키는 URL이다. DID URL은 DID와 함께 사용되어 특정 DID에 연결된 리소스에 대한 참조를 나타낸다. DID URL은 특정 DID Document 내의 공개키, 서비스 엔드포인트 또는 다른 DID와 관련된 정보를 가리키는 데 사용될 수 있다.

#### ① DID URL의 구성요소

- DID URL은 일반적인 URL의 구조를 따르며 DID URL의 일반적인 형식은 다음과 같다

```
did:<method>:<method-specific-identifier>(<specific-ID-parameters>)/<resource>
```

- did: : 프로토콜 명시자(protocol specifier)로서, DID를 식별하는 데 사용된다. 이 부분은 DID의 시작을 나타낸다.
- <method>: 사용된 DID Method를 나타내는 식별자. 예를 들어, eth는 Ethereum DID Method를 의미
- <method-specific-identifier>: 해당 DID Method에 의해 생성된 DID의 식별자
- <specific-ID-parameters>: 특정 DID Method에 대한 추가 매개변수 또는 식별자 관련 매개변수. 선택적이며, DID Method에 따라 상이함
- <resource> : DID와 연결된 리소스의 경로 또는 식별자. DID Document 내의 공개키, 서비스 엔드포인트 등에 대한 참조

#### ② DID URL 사용 예시

```
did:example:123456#keys-1
```

- did:example:123456는 DID를 의미

- #keys-1은 해당 DID Document 내의 특정 공개키를 참조

did:example:123456#service-endpoint

- did:example:123456는 DID를 의미
- #service-endpoint는 해당 DID Document 내의 특정 서비스 엔드포인트 참조

DID URL은 DID를 통해 연결된 여러 리소스에 대한 참조를 쉽게 나타낼 수 있다. DID URL을 사용하면 DID와 관련된 정보를 쉽게 탐색하고 활용할 수 있으며, 분산 식별 체계에서 상호 운용성을 높일 수 있다.

### 3.2.8. Decentralized Key Management System(DKMS)

DIDs의 구성 요소 중 하나인 디센트럴라이즈드 키 매니지먼트 시스템(DKMS)은 사용자 디지털 키를 생성, 저장, 관리한다. 사용자의 신원을 생성, 관리, 인증하는 데 중요한 역할을 하며, 디지털 키는 DID에서 핵심적인 역할을 수행한다.

#### o Decentralized Key Management System (DKMS)의 구성 요소

[표 16] Decentralized Key Management System (DKMS)의 구성 요소

구성 요소	내용
Key Generation (키 생성)	<ul style="list-style-type: none"> <li>- DKMS는 사용자에게 고유한 키 쌍(공개 키 및 비밀 키)을 생성하는데 필요한 알고리즘을 제공</li> <li>- 키 쌍은 사용자의 디지털 식별자를 형성하고, 공개 키는 다른 사용자 또는 시스템과의 안전한 통신에 사용</li> </ul>
Key Storage (키 저장)	<ul style="list-style-type: none"> <li>- DKMS는 안전한 저장소에 키를 보관하고 접근 권한 관리</li> <li>- 데드록스(Decentralized Ledger Technology), 분산원장, 블록체인 등을 활용하여 키를 분산 저장</li> </ul>
Key Rotation (키 회전)	<ul style="list-style-type: none"> <li>- 보안을 유지하기 위해 주기적으로 키 회전 필요</li> <li>- DKMS는 키의 주기적인 갱신을 지원</li> <li>- 키 회전은 기존 키의 유효성을 유지하면서 새로운 키를 생성하고 도입하는 과정</li> </ul>
Access Control (액세스 제어)	<ul style="list-style-type: none"> <li>- DKMS는 키에 대한 액세스를 효과적으로 관리하여 불법 액세스로부터 키를 보호</li> <li>- 사용자가 자신의 키에 외부 액세스를 허용하거나 제한</li> </ul>
Key Recovery (키 복구)	<ul style="list-style-type: none"> <li>- 사용자가 키를 분실하거나 손상된 경우를 대비해 DKMS는 키의 복구 메커니즘을 제공</li> <li>- 분산된 방식으로 키를 저장하기 때문에 여러 지점에서 복구 정보를 가져와 사용자 키를 복원 가능</li> </ul>

o Decentralized Key Management System (DKMS)의 동작 과정

[표 17] Decentralized Key Management System (DKMS)의 동작 과정

프로세스	내용
키 생성	<ul style="list-style-type: none"> <li>- 사용자는 DKMS를 통해 새로운 키 쌍을 생성</li> <li>- 이 키 쌍은 해당 사용자의 식별자를 형성</li> </ul>
키 저장 및 분산	<ul style="list-style-type: none"> <li>- 생성된 키는 안전한 저장소에 저장되며, 분산 네트워크나 블록 체인과 같은 분산원장 기술을 활용해 안전하게 분산</li> </ul>
액세스 및 업데이트	<ul style="list-style-type: none"> <li>- 사용자는 필요할 때마다 자신의 키에 접근하여 업데이트하거나 새로운 키로 회전</li> <li>- 액세스 권한은 사용자가 설정하거나 승인</li> </ul>
액세스 제어 및 복구	<ul style="list-style-type: none"> <li>- 액세스 제어 정책을 적용하여 불법 액세스로부터 보호</li> <li>- 키 복구 메커니즘은 사용자가 키를 손실했을 때 사용</li> </ul>

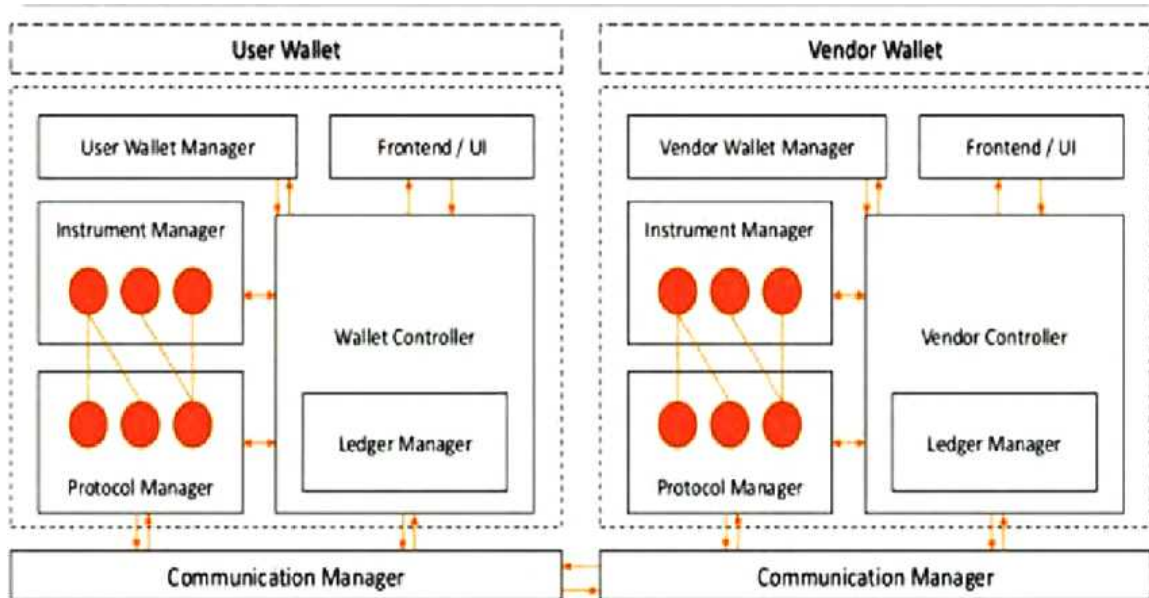
## 제 4 절 Digital Wallet

### 4.1. 개요

디지털 지갑(Digital Wallet)은 모바일 앱이나 웹 애플리케이션과 같은 전자적 형태로 결제, 암호화폐나 중앙은행 디지털 화폐와 같은 디지털 자산을 관리하는데 사용되는 소프트웨어나 애플리케이션이다. 주로 결제 수단을 전자적으로 저장하고 관리하는데 사용되는데 신용 카드, 직불 카드, 은행 계좌 정보, 암호화폐 등 다양한 결제 수단을 안전하게 보관하며, 온라인 및 오프라인에서 결제 편의성을 제공한다. 디지털 지갑은 스마트폰 앱, 웹 애플리케이션, 또는 하드웨어 장치 형태로 제공되며, 생체 인식 기술, 데이터 암호화, 보안 프로토콜 등의 요소 기술을 활용한다.

디지털 지갑의 핵심 요소 기술 중 하나는 강력한 보안 및 암호화 기술인데, 사용자의 결제 정보와 개인 데이터를 안전하게 저장 및 전송하기 위해 SSL/TLS 프로토콜과 같은 암호화 프로토콜이 적용되고 생체 인식 기술인 지문 인식, 얼굴 인식 등이 사용자 인증에 적용되어 높은 수준의 보안을 제공한다.

또한, 디지털 지갑은 지능적인 결제 기능을 위해 NFC(Near Field Communication) 기술을 이용하여 오프라인에서도 간편한 결제를 지원하고 블록체인 기술은 암호화폐 관리 및 안전한 거래를 위한 핵심 기반 기술 중 하나로, 디지털 지갑에서 암호화폐를 보다 효과적으로 관리할 수 있다.



(그림 28) Digital Wallet 아키텍처

#### 4.1. 디지털 지갑의 기반 프레임워크

##### 4.1.1. 보안 및 인증 프레임워크

지문인식, 안면인식 등의 생체 인증 기술, 사용자가 설정한 PIN이나 패턴을 사용하여 접근통제를 설정하고 결제 시에 일회성 토큰을 생성하여 보안성을 강화한다.

##### 4.1.2. 지불 프로토콜

NFC (Near Field Communication)와 같은 근거리 통신 기술을 활용하여 무선으로 지불이 가능하도록 하고 가맹점과의 결제를 위한 QR 코드나 바코드, 다양한 Pay 시스템과의 연동을 위해 모바일 결제 플랫폼과 연동하기 위한 지불 프로토콜을 사용한다.

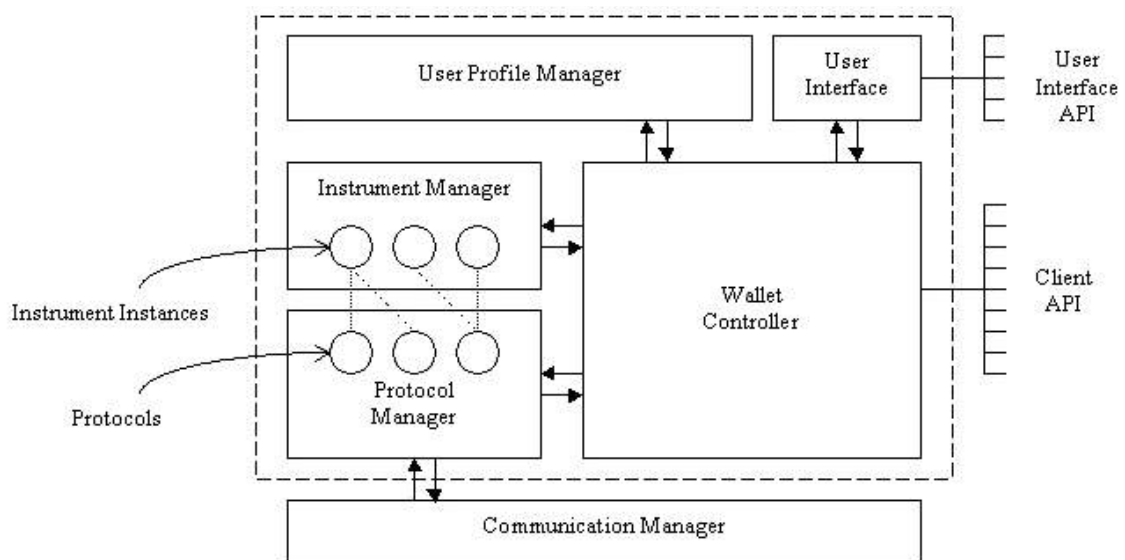
##### 4.1.3. 블록체인 기술

블록체인을 활용하여 프로그래밍 가능한 스마트 계약을 통해 보다 안전하고 효율적인 거래를 지원하고 분산원장 기술을 활용하여 거래 내역이 블록체인에 기록되어 중앙화된 데이터 저장소 없이도 안전하게 관리하도록 지원한다.



## 4.2. 디지털 지갑의 구성요소

사용자 인터페이스, Wallet Controller, Protocol Manager, Secure Element (보안 요소), Payment Gateway Integration 등으로 구성되며 안전하고 효율적인 디지털 지갑 서비스를 제공한다.



(그림 29) Digital Wallet 구성요소

### 4.2.1. Wallet Controller

사용자 요청을 해석하고 결제 처리, 알림 발송 등 핵심로직을 처리하고 인터페이스와 백엔드 시스템 및 외부 결제 서비스와의 상호 작용을 관리한다.

[표 18] Wallet Controller의 주요 기능

기능	내용
사용자 인터페이스 관리	디지털 지갑 애플리케이션에서 사용자와 상호작용하며 사용자의 요청을 수신
지갑 로직 처리	결제, 잔액 조회, 거래 기록 확인 등 핵심 지갑 기능을 수행
결제 서비스 통합	외부 결제 서비스와 통합하여 결제 요청과 결과 처리
보안 및 권한 관리	사용자 인증 및 권한 부여를 통해 안전한 지갑 사용을 보장
이벤트 처리 및 알림	거래 완료, 잔액 변경 등의 이벤트를 감지하고 사용자에게 알림을 제공
로그 및 감사	시스템 동작 및 사용자 활동에 대한 로그를 생성하여 감사 및 모니터링을 지원

사용자가 디지털 지갑 애플리케이션을 통해 결제 요청이나 기타 기능을 호출하면 Wallet Controller는 사용자의 요청을 받아들이고 해당 요청에 필요한 지갑 로직을 처리하기 위해 내부서비스 및 데이터에 접근한다. 필요에 따라 외부 결제 서비스와 통신하여 결제를 진행한 후 지갑의 상태를 업데이트하고 사용자에게 결과와 알림을 제공하며, 필요한 경우 사용자 인터페이스를 업데이트하여 새로운 정보를 표시한다.

#### 4.2.2. Protocol Manager

Protocol Manager는 외부 시스템과의 통신을 관리하는 역할을 수행하며, 다양한 프로토콜을 지원한다.

[표 19] Protocol Manager의 주요 기능

기능	내용
프로토콜 관리	프로토콜을 관리하고 외부 시스템 및 서비스와 통신 수행
보안 프로토콜 구현	안전한 통신을 위한 보안 프로토콜을 구현 및 관리
데이터 변환 및 인코딩	다양한 데이터 형식 및 인코딩 방식에 대한 변환을 수행하여 시스템 간의 호환성을 유지
외부 API 및 서비스 연동	외부 시스템 및 서비스와의 통신을 담당

외부 결제 서비스, 은행 API, 암호화폐 거래소 등 외부서비스와의 통신을 위해 필요한 프로토콜을 선택하고 구현하며, 보안 프로토콜을 활용하여 안전한 통신을 보장하고, 필요에 따라 데이터의 변환 및 인코딩을 수행하여 시스템 간의 데이터 교환을 원활하게 한다. Wallet Controller에서 발생한 요청에 대한 외부 서비스의 응답을 해석하고 Wallet Controller에 전달하여 지갑 로직을 완료한다.

#### 4.2.3. User Profile Manager(사용자 프로필 관리자)

User Profile Manager(사용자 프로필 관리자)는 디지털 지갑 시스템에서 사용자 정보를 관리하고 유지하는 역할을 수행하는 구성 요소 중 하나로 사용자 중요정보를 저장하고, 지갑 서비스를 개인화하며 보안을 강화하는 역할을 한다.

[표 20] User Profile Manager의 주요 기능

기능	내용
사용자 등록 및 관리	<ul style="list-style-type: none"> <li>- 새로운 사용자가 디지털 지갑 서비스에 가입할 때, 해당 사용자의 정보를 수집하고 등록</li> <li>- 사용자 정보는 고유한 식별자, 기본 정보(이름, 이메일 등), 보안 관련 정보(비밀번호, 생체 인식 정보 등) 등</li> </ul>
프로필 업데이트	<ul style="list-style-type: none"> <li>- 사용자가 프로필 정보를 변경하거나 업데이트할 때, 변경 사항을 적용하고 저장</li> </ul>
보안 및 인증 관리:	<ul style="list-style-type: none"> <li>- 비밀번호, PIN, 생체 인식 정보(지문, 얼굴 인식 등) 등의 인증 수단을 포함한 사용자 보안정보를 안전하게 관리</li> <li>- 보안 정책을 준수하고 사용자 계정의 안전성을 유지하기 위해 사용자의 인증 정보를 안전한 방식으로 저장합니다.</li> </ul>
알림 및 통지 관리	<ul style="list-style-type: none"> <li>- 사용자에게 중요한 알림이나 통지를 전송할 때 사용되는 거래 완료, 계정 상태 변경, 보안 이슈와 같은 정보 관리</li> </ul>
비즈니스 인텔리전스 지원	<ul style="list-style-type: none"> <li>- 사용자 프로필에 저장된 정보를 기반으로 사용자의 화폐 설정, 선호도, 거래 기록 등을 고려하여 사용자 경험을 최적화하는 비즈니스 인텔리전스를 제공</li> </ul>

#### 4.2.4. Instrument Manager

Instrument Manager(금융 상품 관리자)는 디지털 지갑 시스템에서 다양한 금융 상품 및 결제 수단을 관리하고 효율적으로 처리하는 역할을 수행하는 구성 요소 중 하나이다. 다양한 결제 수단과 금융 상품을 통합하고 관리하여 사용자에게 편리하고 다양한 옵션을 제공하는 데 중요한 역할을 한다.

[표 21] Instrument Manager의 주요 기능

기능	내용
금융 상품 관리	<ul style="list-style-type: none"> <li>- 신용카드, 직불카드, 은행 계좌, 전자화폐, 암호화폐 등 다양한 결제 수단을 통합하여 사용자에게 제공</li> <li>- 수수료, 환율, 할인 혜택, 결제 한도, 거래 내역 등 각 금융 상품에 대한 정보를 사용자에게 제공</li> <li>- 사용자의 거래 이력과 선호도를 기반으로 금융 상품을 추천하고 혜택을 제공</li> <li>- 사용자 경험을 향상시키고 서비스 이용을 증진</li> </ul>
결제 수단 등록 및 해지	<ul style="list-style-type: none"> <li>- 사용자가 새로운 결제 수단을 등록하거나 이전에 등록한 결제 수단을 해지하는 등의 요청 처리</li> <li>- 등록된 결제 수단에 대한 유효성 검사와 보안 절차를 수행</li> </ul>
결제 처리 및 통합	<ul style="list-style-type: none"> <li>- 결제 수단을 지원하고 외부 결제 서비스와의 연동 관리</li> <li>- 사용자가 결제를 요청하면 적절한 결제 수단을 식별하고 해당 결제를 처리</li> </ul>

#### 4.2.5. Communication Manager(통신 관리자)

디지털 지갑 시스템에서 다양한 시스템 및 외부 서비스와의 효율적인 통신을 관리한다. 지갑 내부의 여러 모듈 및 외부 서비스 간의 통신을 조정하고 안전한 데이터 전송을 보장하여 원활한 서비스 운영을 지원한다.

[표 22] Communication Manager의 주요 기능

기능	내용
내부 모듈 간 통신 관리	<ul style="list-style-type: none"> <li>- 지갑 내의 여러 모듈(예: Wallet Controller, Protocol Manager, User Profile Manager 등) 간 통신 조정</li> <li>- 각 모듈 간에 필요한 데이터 및 이벤트를 전송하고 수신</li> </ul>
외부 서비스와의 통신 관리	<ul style="list-style-type: none"> <li>- 외부 서비스와 통신을 관리하고 안전하게 상호 작용</li> <li>- 외부 결제 게이트웨이, 은행 API, 암호화폐 거래소 등과의 통신을 조정</li> <li>- 안전한 통신을 위해 암호화, 기타 보안 프로토콜을 구현하고 관리</li> <li>- 사용자의 개인 정보 및 금융 데이터를 안전하게 전송하기 위한 보안 조치</li> </ul>
프로토콜 관리 및 변환	<ul style="list-style-type: none"> <li>- 다양한 통신 프로토콜을 관리하고 필요한 경우 프로토콜 간 변환을 수행하여 호환성을 유지</li> </ul>

#### 4.3. Digital Wallet의 처리 흐름

사용자의 요청부터 결제 완료 및 알림까지의 모든 단계를 처리하기 위해 주요 구성 요소 간에 상호 작용하는 프로세스가 수행되어 안전하고 효율적인 디지털 지갑 서비스를 제공한다.

[표 23] Digital Wallet의 처리 흐름

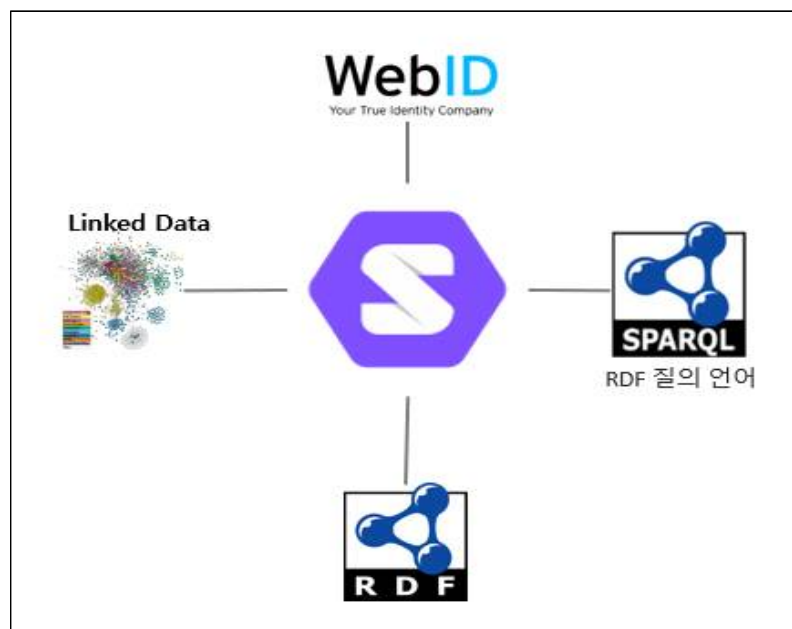
단계	내용
사용자 요청 및 인터페이스	<ul style="list-style-type: none"> <li>- 사용자가 모바일 애플리케이션 또는 웹 인터페이스를 통해 디지털 지갑에 액세스하고 서비스 요청</li> <li>- 결제, 송금, 잔액 조회 등 사용자 요청을 Wallet User Interface를 통해 전달</li> </ul>
Wallet Controller 처리	<ul style="list-style-type: none"> <li>- 계좌 정보조회, 거래내역 조회 등 사용자의 요청을 받아들이고 지갑의 핵심 로직 수행</li> <li>- 결제 요청인 경우, 사용자의 결제 정보를 확인하고 해당 거래를 처리</li> </ul>
User Profile Manager 처리	<ul style="list-style-type: none"> <li>- User Profile Manager를 통해 사용자 프로필 정보 확인</li> <li>- 사용자 정보, 보안 인증 정보, 등록된 결제 수단 등이 User Profile Manager에 저장</li> </ul>
Instrument Manager 처리	<ul style="list-style-type: none"> <li>- Wallet Controller는 결제 요청에 따라 Instrument Manager를 통해 등록된 결제 수단을 확인하고 처리</li> <li>- Instrument Manager는 결제에 사용될 수 있는 모든 금융</li> </ul>

	상품 및 결제 수단을 관리하고 지원
Communication Manager 통신	<ul style="list-style-type: none"> <li>- Wallet Controller는 외부 서비스와의 통신이 필요한 경우 Communication Manager를 통해 통신</li> <li>- 결제 게이트웨이, 은행 API, 암호화폐 거래소 등과의 통신은 Communication Manager가 관리</li> </ul>
결제 수단 및 금융 상품 관리	<ul style="list-style-type: none"> <li>- Instrument Manager는 결제 요청에 대한 결제 수단의 유효성을 검사하고, 사용자의 금융 상품 정보를 확인</li> <li>- 사용자가 지정한 결제 수단에 따라 결제가 처리되고, Instrument Manager는 결제 상태를 업데이트</li> </ul>
Notification Service 알림 발송	<ul style="list-style-type: none"> <li>- 결제가 성공적으로 처리되거나 중요 이벤트가 발생하면, Notification Service를 통해 사용자에게 알림이 전송</li> </ul>
Logging and Auditing 기록 및 감사	<ul style="list-style-type: none"> <li>- 중요한 이벤트와 사용자 활동을 Logging and Auditing 모듈을 통해 기록하고 감사</li> </ul>

## 제 5 절 Solid Project

Solid(Social Linked Data)는 월드와이드웹의 발명가인 팀버너스리가 주도하는 웹 탈중앙화 프로젝트로 MIT와 협업하여 개발되었다. Solid의 궁극적인 목표는 사용자들이 자신만의 데이터를 온전히 통제하게 할 수 있는 것이다.

다음 그림은 Solid의 구성요소를 나타내고 있다. Solid는 WebID, Linked Data 플랫폼, RDF, SPARQL 등 여러 웹 표준을 일관성있게 결합하여 제시한다.



(그림 30) Solid 구성요소

## 1. Solid 구성요소

### 1.1 WebID

WebID는 URI를 사용하여 사람, 회사, 조직 또는 기타 에이전트를 고유하게 식별하는 방법이다. 또한 WebID는 서비스에 의해 노출된 정보를 휴대가능하고 미래에 대비할 수 있는 방식으로 함께 묶는데 사용할 수 있는 식별자이다.

WebID 그룹의 대표인 WebID Solutions GmbH는 자금세탁법(GwG)을 준수하는 비디오 식별의 발명자이자 선구자로서 혁신의 원동력이자 온라인 식별 서비스 분야의 유럽 최대 기업 중 하나이다. 여기에는 비디오 식별 외에도 디지털 신원(True Identity), 자동 연령 확인, 법적으로 유효한 온라인 서명 프로세스 및 기타 여러 솔루션이 포함된다. 2012년에 설립된 이 회사는 1억 8천만 개가 넘는 신분증 데이터 필드의 진위 여부를 확인하고 해당 사용자를 식별하였다. WebID 비디오 식별의 품질과 높은 수용성 덕분에 사용자의 이익을 위한 “진정한 신원”의 안전한 저장 및 재사용 모델은 WebID 창립 이후 구현되어 그 자체로 입증되었다. 사용자의 요청에 따라 WebID는 확인된 실제 신원을 보관하는 역할을 하여 일상적인 신원 확인 또는 온라인으로 법적으로 준수하는 계약 종료 시 더 좋고 매우 안전한 사용자 경험을 제공한다.

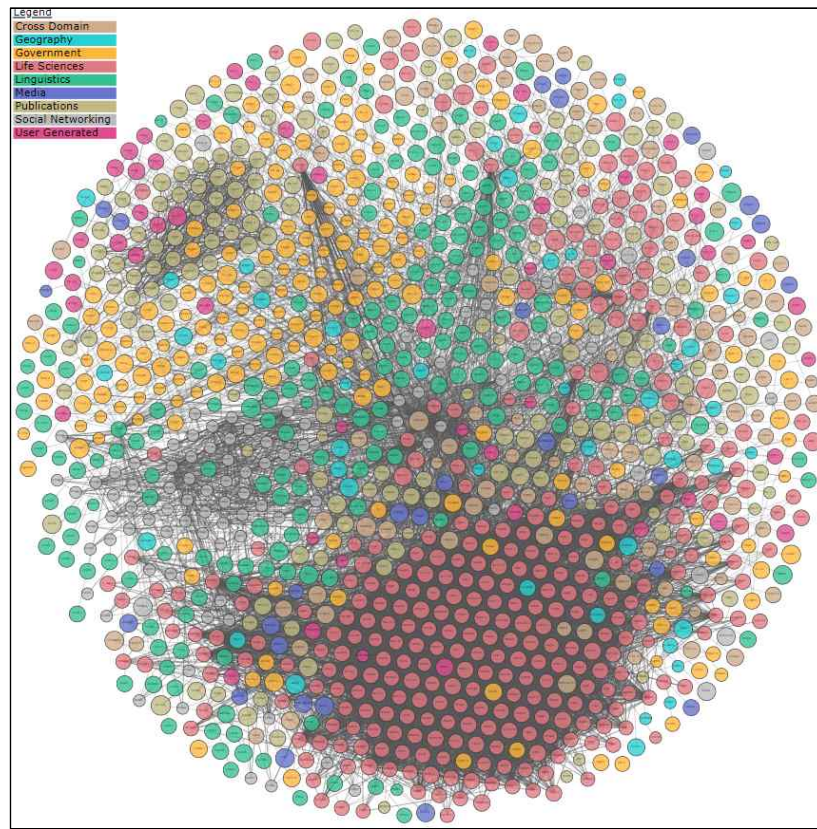


(그림 31) WebID 솔루션

### 1.2. Linked Data

Linked Data는 웹 상에 존재하는 데이터를 개별 URI로 식별하고 각 URI에 링크 정보를 부여하여 상호 연결된 웹을 지향하는 모형이다. 데이터의 웹은 웹 상의 문서로 구성되며 RDF에 의해 설명된 임의의 항목간에 데이터를 연결한다.





(그림 32) lod-cloud.net에 연결된 개방형 데이터 클라우드

Linked Data의 4 원칙은 다음과 같다.

- o URI의 사용: 링크드 데이터는 웹문서의 위치를 나타내는 URL 중심의 식별체계를 지양한다. 즉, 개별 문서에 존재하는 개별 객체에 각각 URI를 부여하는 것이다.
- o HTTP URI의 사용: 링크드 데이터는 URI 중에서도 HTTP 프로토콜을 통해 접근할 수 있는 URI를 제안하고 있다. 이는 링크드 데이터에 대한 접근성을 강화하려는 목적이다.
- o RDF의 사용: 링크드 데이터는 RDF와 같이 트리플 모형으로 구조화된 데이터를 사용해야 한다. 웹의 데이터를 정형화된 구조로 나타내고, 연계하기 위해서이다.
- o 링크정보의 부여: 위의 세 가지 원칙을 지켰다고 해도, 풍부한 링크정보가 없다면 웹에 존재하는 데이터를 연결하기는 어려울 것이다. 기존의 시맨틱웹에서도 링크 정보를 부여할 수는 있었으나, 그 보다는 구조화된 표현(3번과 같이)을 주로 강조했었다. 링크드 데이터에서는 보다 발전된 시맨틱웹을 위해 링크정보를 부여하는 것이 매우 중요하다.

### 1.3. RDF(Resource Description Framework)

RDF는 W3C 표준으로, 웹 페이지의 제목, 저자, 수정일, 내용과 같은 웹 자원을 표시하기 위한 것이다. 주어, 서술어 목적어로 이루어진 트리플로 표현한다.

Ex) 보노보는 포유류이다.

dbpedia:Bonobo      rdf:type      dbpedia-owl:Mammal

주어

서술어

목적어

주어에는 **서술어**가 있는데 그 값은 **목적어**이다.

### 1.4. SPARQL

SPARQL(“sparkle“, 스파클, SPARQL Protocol and RDF Query Language의 재귀 약자)은 RDF 질의어, 즉 데이터베이스를 위한 시맨틱 질의어로서 자원 기술 프레임워크(RDF) 형식으로 저장된 데이터를 검색, 조작할 수 있다. 월드 와이드 웹 컨소시엄의 RDF DAWG(Data Access Working Group)에 의해 표준화되었으며 시맨틱 웹의 주요 기술 가운데 하나로 지목된다. 2008년 1월 15일, SPARQL 1.0은 공식 W3C 권고안이 되었으며, 2013년 3월 SPARQL 1.1이 그 다음 권고안으로 되었다. SPARQL은 쿼리가 트리플 패턴, 논리곱, 논리합, 선택적 패턴을 구성할 수 있게 한다. 여러 프로그래밍 언어를 위한 구현체들이 존재한다. 이를테면 ViziQuer처럼 SPARQL 엔드포인트를 위한 SPARQL 쿼리를 연결, 반자동 구성할 수 있게 하는 도구들이 존재한다. 이뿐 아니라 SPARQL 쿼리를 다른 질의어, 즉 SQL과 XQuery로 변환하는 도구들도 존재한다.

Ex) “아프리카의 모든 국가 수도는?”이라는 질문의 SPARQL 쿼리 예제

PREFIX ex: <http://example.com/exampleOntology#>

SELECT ?capital

      ?country

WHERE

{

  ?x ex:cityname        ?capital ;

     ex:isCapitalOf    ?y .

  ?y ex:countryname    ?country ;

     ex:isInContinent ex:Africa .

}



## 2. Solid 프로젝트

솔리드 프로젝트의 목적은 웹 애플리케이션이 동작하는 방식을 근본적으로 변화시킴으로써 진정한 데이터 소유권을 가지고 프라이버시 개선을 이루는 것으로, 이는 탈중앙화 되어 온전히 사용자의 통제를 받는 Linked Data 애플리케이션 플랫폼을 개발하여 이루어진다.

### 2.1. Solid, Pod

Solid는 사람들이 Pod라는 분산형 데이터 저장소에 데이터를 안전하게 저장할 수 있는 플랫폼으로, Pod는 데이터를 저장하기 위한 안전한 개인 웹 서버이다. 모든 종류의 정보를 Solid Pod에 저장할 수 있고, Pod의 데이터에 대한 접근을 제어하고 데이터를 누구와 공유할 것인지 결정(개인, 조직, 애플리케이션) 한다. 언제든지 접근 권한을 철회할 수 있고, Pod에 데이터를 저장하고 접근하기 위해 애플리케이션은 상호운용가능한 표준 개방형 데이터 형식과 프로토콜을 사용한다.

Solid, Pod에는 다음과 같은 규칙이 있다.

- o Solid Server는 하나 이상의 Solid Pod를 호스팅한다.
- o Pod는 데이터를 저장하는 위치이다.
- o 각 Pod는 Pod 소유자(즉, 본인)가 완전히 제어한다.
- o 각 Pod의 데이터 및 접근 규칙은 다른 Pod의 데이터 및 규칙과 완전히 다르다.
- o Pod 제공자로부터 Pod를 받거나 Pod를 자체 호스팅하도록 선택할 수 있다.
- o Pod를 여러 개 가질 수 있다.
- o Solid에서 데이터는 ID를 통해 연결되므로 투명한 연결이 가능하다.

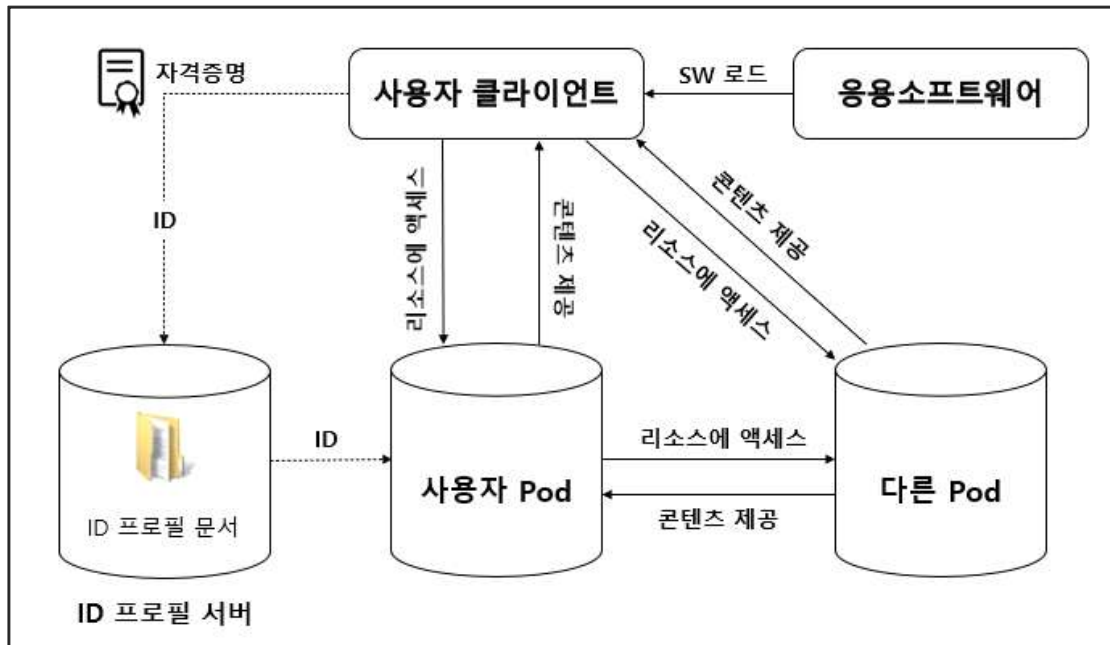
### 2.2. Solid 아키텍처

Solid 아키텍처의 동작과정과 내용은 다음과 같다.

- o 사용자는 자신의 ID를 RDF 프로필 문서를 사용하여 제어하며, 이는 일반적으로 Pod 서버에 저장된다.
- o 사용자는 애플리케이션 제공자로부터 Solid 애플리케이션을 로드한다.
- o 애플리케이션은 ID프로필에서 사용자의 Pod을 얻는다.

- o 그런 다음 프로필에서 링크를 따라 사용자 Pod뿐만 아니라 다른 Pod에 대한 데이터를 발견하며, 필요할 때 인증을 수행한다.

다음 그림은 Solid 아키텍처 구성도를 보여준다.



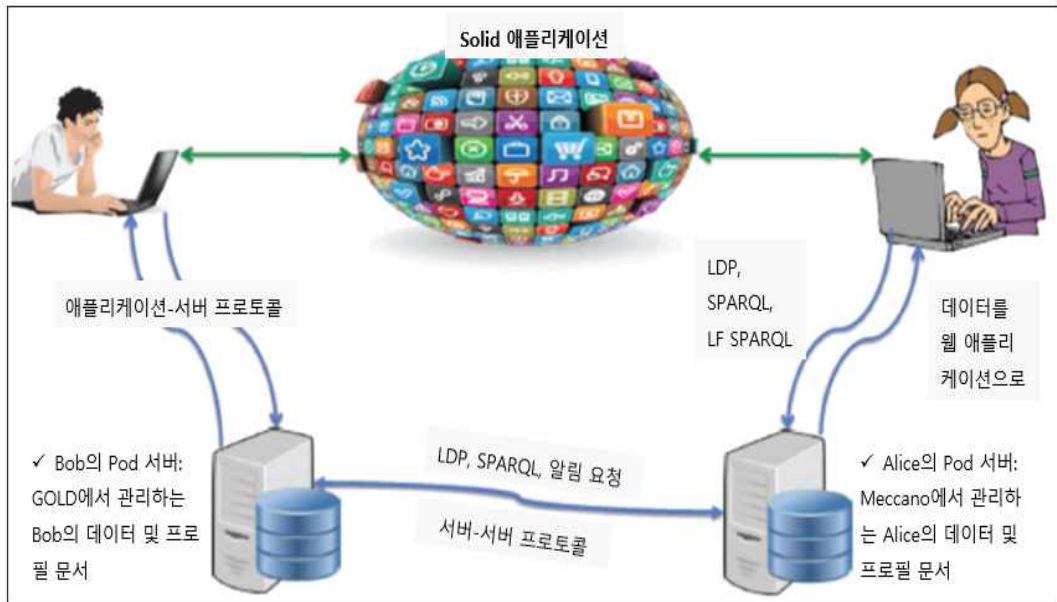
(그림 33) Solid 아키텍처 구성도

Solid 아키텍처에서 WebID-TLS는 클라이언트 인증서를 공개키 인증을 수행하는 수단으로 사용된다. 인증서의 공개키를 WebID를 참조하여 얻은 프로필 문서에 나열된 공개키와 일치하는지 확인하고, WebID로 에이전트가 고유한 식별자를 HTTP(S) URI 형식의 프로필 문서에 연결하여 자신의 ID를 생성한다. 공개·비공개 방식으로 프로필을 연결할 수 있는 웹 신뢰의 모든 필요한 정보가 포함되어 있다. WebID 인증서(자격증명)를 선택만 하면 인증이 이루어진다.

### 2.3. Solid 플랫폼

Solid를 지원하는 애플리케이션 및 서버 세트를 통해 Solid가 애플리케이션 간의 높은 상호 운용성, 데이터 및 소셜 그래프의 쉬운 공유, 그리고 서버 간의 데이터 이식성을 가능하게 한다.

다음 그림은 Solid 플랫폼 예시를 보여준다.

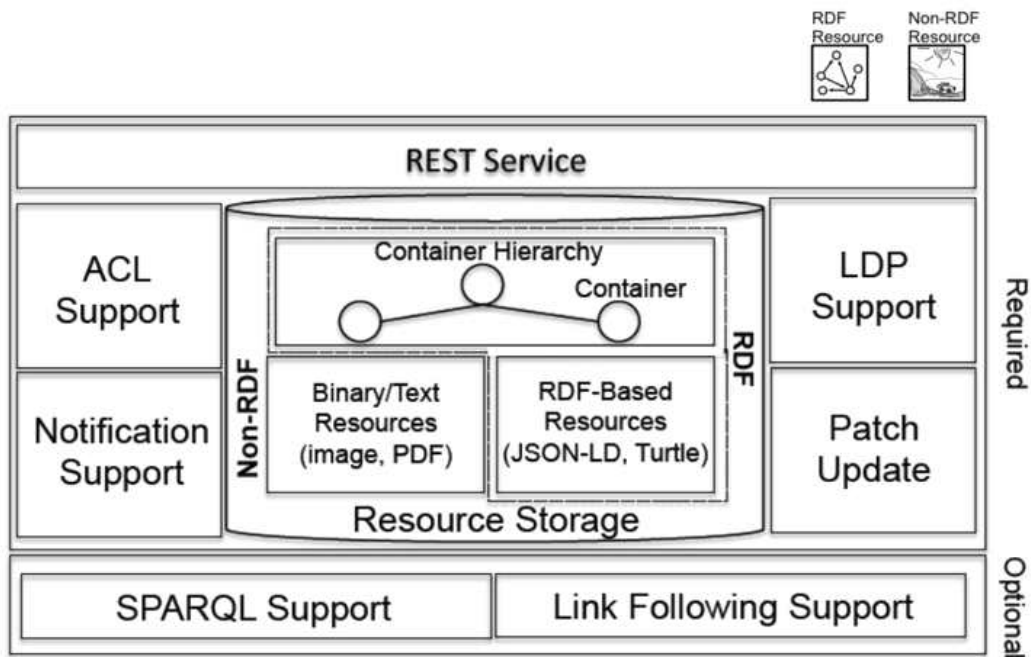


(그림 34) Solid 플랫폼 예시

## 2.4. Pod 아키텍처

Pod은 RDF 및 비-RDF 리소스를 저장하고, Pod 서버는 LDP, 리소스 패치, 접근 제어, 실시간 업데이트를 지원하며 선택적으로 SPARQL을 지원한다.

다음 그림은 Pod 아키텍처의 구조를 보여준다.



(그림 35) Pod 아키텍처

Pod 아키텍처의 구성요소는 다음과 같다.

- o **리소스 저장소**: RDF 데이터의 기본 저장방식은 파일시스템, 키-값 저장소, 관계형 DBMS, 그래프 DBMS를 사용할 수 있다.
- o **LDP지원, 패치 업데이트**: Pod는 기본 LDP 작업(HTTP GET, POST, DELETE, OPTIONS 및 HEAD)와 LDP 확장을 지원한다. SPARQL쿼리를 사용하여 패치작업을 수행한다.
- o **접근제어**: 웹접근제어(WAC) 온톨로지를 사용하여 접근 제어를 수행한다. (Read, Write, Control, Append 모드)
- o **SPARQL 지원**: 복잡한데이터 검색을 위해 선택적으로 SPARQL을 지원한다.

## 제 4 장 Trusted Web 설계

### 제 1 절 Trusted Web 아키텍처 설계

#### 1. Trusted Web 아키텍처 설계 원칙

Trusted Web은 인터넷과 웹을 기반으로 하는 디지털 사회의 통신 기반에서 신원 관리에 중점을 둔다. Trusted Web의 목표는 디지털 사회에서 새로운 트러스트 프레임워크를 구축하여 다양한 사회활동에 대응하는 것이다. Trusted Web의 기능은 사용자(개인 및 조직)가 자신의 데이터를 효과적으로 제어할 수 있도록 하고, 특정 서비스에 지나치게 의존하지 않으면서도 데이터 교환에서 합의를 구축하고 해당 합의를 추적할 수 있는 메커니즘을 통합하는 것이다. 이를 통해 검증 가능한 영역을 확대하고 신뢰 수준을 향상시킨다.

Trusted Web은 블록체인과 같은 다양한 기술을 융합하여 이를 실현할 수 있으며, 동시에 현재의 인터넷 아키텍처와의 연속성, 기존 시스템과의 상호 운용성, 그리고 업그레이드 용이성을 보장한다.

Trusted Web의 구현은 인터넷과 웹의 기존 장점을 활용하면서도, 위에서 언급한 기능 요구사항을 추가하는 오버레이 접근법을 사용한다. 이는 기존 시스템이나 구조 위에 새로운 계층이나 모듈을 적용하는 방식으로 이루어진다. 이러한 접근법을 통해 Trusted Web은 현대의 디지털 환경에서 신뢰성 있고 효율적인 신원관리를 제공하도록 한다.

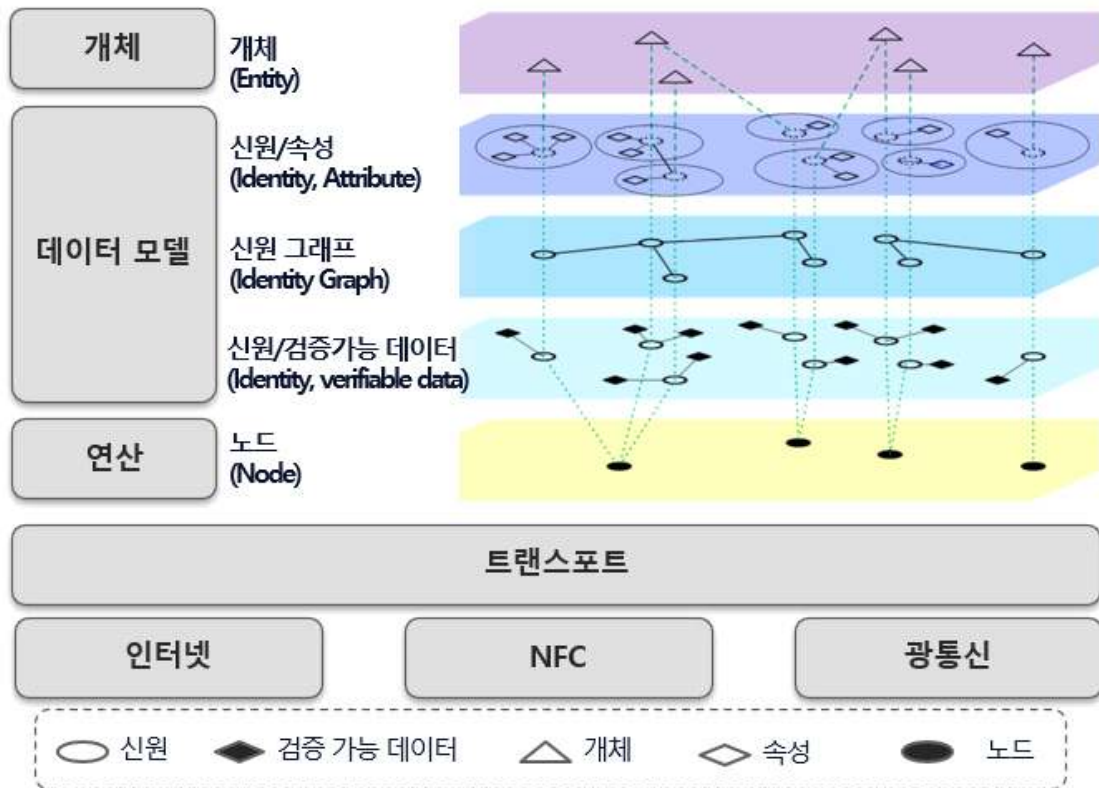
#### [ Trusted Web 아키텍처 설계 원칙 ]

- 신원관리(Credential) 중심의 개체 및 데이터 검증
- 자기 정보(데이터, 개인정보 등) 주권 보장
- 특정 플랫폼 서비스의 종속성 탈피
- 거래 공정성을 위한 데이터 추적과 검증
- 특정 기술에 의존적이지 않으면서 다양한 기술 수용
- 현 인터넷 아키텍처와의 연승성, 상호 운용성, 업그레이드 용이성

## 2. Trusted Web Architecture 계층 구조 및 구성요소

Trusted Web 아키텍처 설계원칙을 보장하기 위해 Trusted Web의 아키텍처 구성 요소는 검증 가능한 데이터, ID, 노드, 메시지, 트랜잭션, 전송수단으로 구성한다.

다음 그림은 Trusted Web Architecture의 계층적 구조를 보여준다.



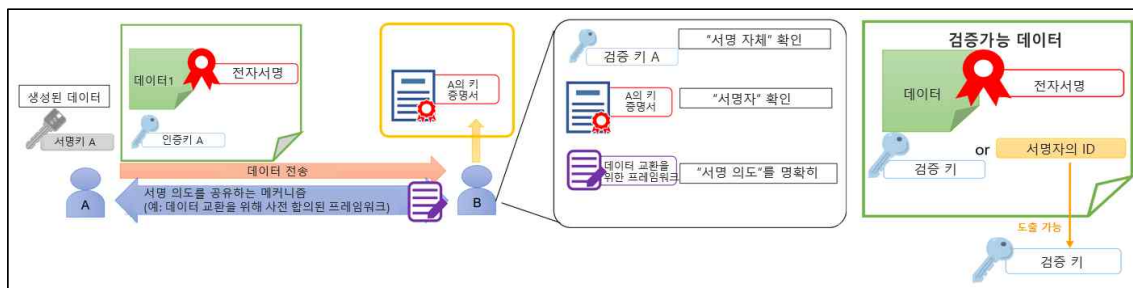
(그림 36) Trusted Web Architecture

- 개체(Entity): 개체는 참여자로 사용자 또는 어플리케이션 등이 될 수 있다.
- 신원(Identity): 검증 가능한 데이터의 일종으로 속성으로 구성된다. 이러한 데이터를 만들기 위해서는 이를 ID와 관련된 서명에 관한 정보와 연결하고 ID 간의 관계를 나타내는 ID 그래프를 참조하는 것이 필수적이다. 이는 데이터의 검증 가능성을 확대하는데 도움이 된다.
- 속성(Attribute): 속성은 신원이 가지고 있는 특성을 의미한다. 개체의 역할, 권한, 자격정보, 거래권한 등이 속성정보로 활용된다. 개체의 속성정보는 크리덴셜(ID)를 생성하기 위한 재료로 활용된다.
- 신원그래프(Identity Graph): 개체의 디지털 신원에 관한 정보를 효과적으로 관리

- 하고 연결하는 데 사용되는 그래프 형태의 자료구조이다. 이 그래프는 사용자의 다양한 디지털 신원정보를 서로 연결하여 사용자의 신원을 통합하고 표현한다.
- **검증 가능한 데이터:** Trusted Web에서 작동되는 데이터로 “서명 “, “서명자” , “서명의 의도” 를 확인함으로써 서명이 포함된 전체 데이터를 확인할 수 있다.
  - **노드:** 메시지를 보내고 받는 일을 담당한다. 메시지 수신 시 계산 처리(예:합의형성)를 수행 할 수 있다. 노드는 거래를 기록하고 기록은 ID와 연결되어 유지된다.
  - **메시지:** 소스에서 대상까지 확실하게 전달되는 단방향 메시지 전송이다. 노드 간에 데이터를 교환하고 노드에서 구현한다.
  - **트랜잭션:** 노드가 노드 간의 메시지 교환 순서를 확인할 수 있도록 하는 데이터 및 메커니즘으로 이는 분산 저장을 보장하고 모든 노드가 기록을 유지하도록 보장한다. 외부 기록에 의존하지 않으며 비밀유지 방식으로 관련 당사자 간에만 공유할 수 있다.
  - **전송 수단:** 다른 노드에 메시지를 보내는 적절한 수단을 제공한다. 인터넷, 근접 기반 무선통신 등 다양한 기술을 적용하기 위해서는 종합적인 통신 모델이 필요하다.

## 2.1. 검증가능 데이터

검증가능 데이터 모델은 데이터, 데이터에 대한 디지털 서명, 검증 키 또는 검증 키가 파생될 수 있는 신원, 서명의 의도(의도를 데이터로 나타낼 수 있는 경우)이다. 고급 데이터 처리 방법으로 자격 증명 및 안전한 계산(데이터를 암호화한 상태로 다양한 유형의 분석을 가능하게 하는 기술)과 같은 고급 암호 처리 방법이 제안되고 있다. 이러한 처리 방법은 검증 가능한 데이터를 위해 도입될 수 있지만, Identity 작업과 결합되는 것으로 인식된다.



(그림 37) 검증가능 데이터 작업의 예시

검증 가능한 데이터의 작업은 A가 B에게 데이터를 전송하는 과정에서 발생한다. A는 전송할 데이터를 생성(생성된 데이터)하고, 자신의 서명키(서명키 A, Private Key A)로 디지털 서명을 하여 데이터와 함께 전송한다. 전자서명 과정에서는 데이터에 대한 해시값에 디지털 서명(비대칭키 암호화) 방식을 사용한다.

데이터를 수신한 B는 A의 키 증명서에서 검증키(Public Key A)를 추출하여, A로부터 수신한 데이터에 대한 진본성을 확인한다. 데이터 검증은 양측간 사전에 협의된 데이터 교환 프로토콜을 정의하여 사용한다.

## 2.2. 신원, 속성, 신원 그래프

디지털 신원(ID)의 데이터 모델은 디지털 서명과 기타 속성으로 이루어져 있으며, 서명, 검색, 서명검증을 위한 데이터 획득, 고급 데이터 처리 등의 작업을 수행한다. 이와 별도로 ID 그래프는 각 ID를 노드로 표현하고, 일대일 관계를 선으로 연결하는 그래프 구조를 가지며, ID 간의 관계 추가, 삭제, 업데이트, 경로 찾기, 검증 가능성 평가 등의 작업을 수행한다.

두 데이터 모델은 서로 독립적으로 작동하면서도 디지털 환경에서 신원의 관리와 투명성을 높이기 위해 협력한다. ID 그래프는 데이터의 검증 가능성을 경로를 통해 평가하여 디지털 추적 및 신뢰성 제고에 기여한다.

ID의 작업항목과 내용은 다음과 같다.

- o 서명: Identity와 연결된 서명 키로 서명이 가능하다.
- o 검색: Identity는 일정한 방법으로 검색이 가능하다.
- o 서명의 검증을 위한 데이터 획득: Identity와 연결된 키(검증키)가 필요하다.
- o 서명자의 확인을 위한 데이터 획득: 검증키로부터 서명키의 소유자를 확인하고 검증한다.
- o 고급 데이터 처리: 고급 암호화 기술이 구현된 경우, 관련된 작업을 구현한다.

ID 그래프의 데이터 모델은 ID를 노드로 일대일 관계를 선으로 갖는 그래프로 각 ID는 자신의 ID 그래프를 관리한다. 구성요소는 ID, Identity 식별 데이터(예: 식별자), Identity 간의 관계를 나타내는 데이터이다.

ID 그래프의 작업은 다음과 같다.

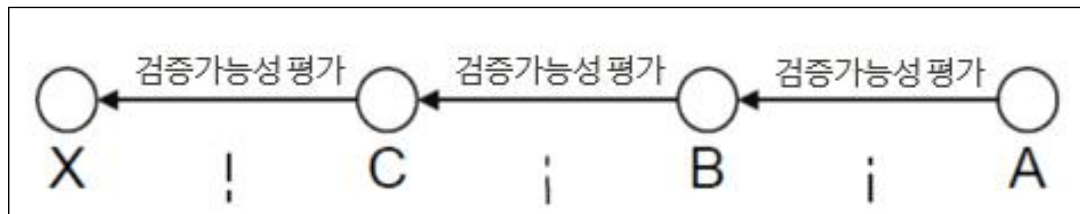
- o ID 간의 관계 추가



- o ID 간의 관계 삭제
- o ID 간의 관계 업데이트
- o 경로 찾기
- o 경로의 검증 가능성 평가

ID 그래프는 검증해야 할 데이터와 서명을 한 Identity로 연결 가능하며 노드와 선의 조합은 “경로” 라고 한다. 경로를 이루는 라인의 검증 가능성을 평가함으로써, 경로 전체의 검증 가능성을 평가할 수 있으며, 결국 추적의 종점에 있는 Identity가 제공한 데이터의 검증 가능성을 평가할 수 있다.

다음 그림은 전체 경로의 검증 가능성 평가를 도식화 한 것이다. B가 제공한 데이터에 대해 A는 C와 X가 제공한 데이터의 검증 가능성을 평가한다.



(그림 38) 전체 경로의 검증 가능성 평가

### 2.3. 노드, 메시지, 트랜잭션, 전송

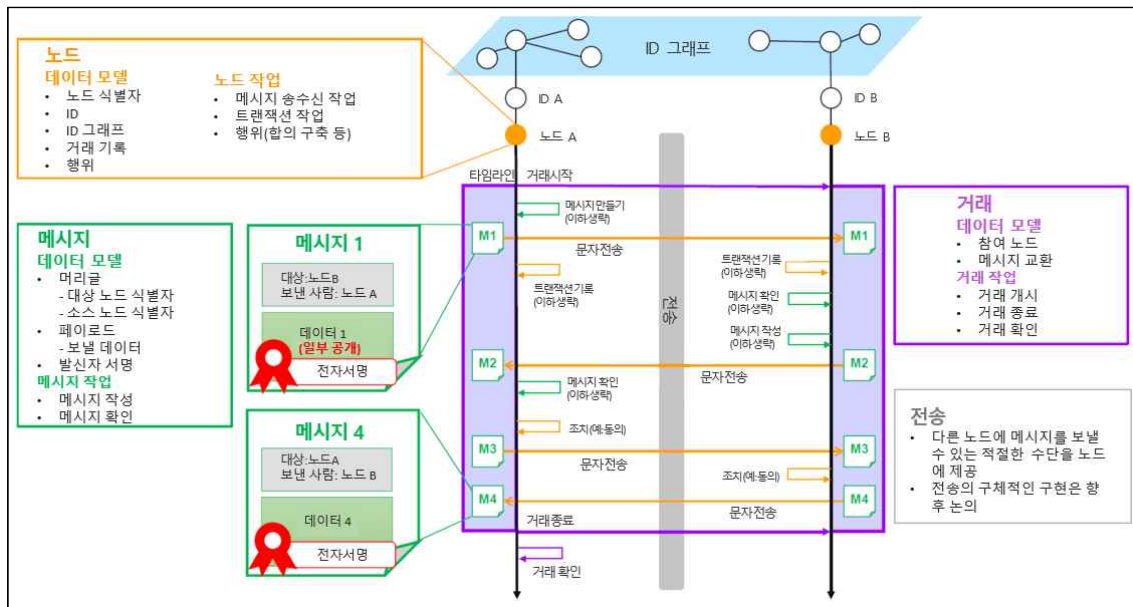
노드는 메시지를 보내고 받는 일을 담당하고 합의형성을 수행하며 거래를 기록한다. 노드의 데이터 모델은 노드 식별자, ID, ID 그래프, 거래기록, 행위로 구성되고 노드의 작업은 메시지 송수신 작업, 트랜잭션, 합의 구축 등이 있다.

메시지는 소스에서 대상까지 단방향 메시지(Hash Message)를 전송한다. 메시지의 데이터 모델은 노드 식별자, 보낼 데이터, 발신자 서명으로 구성되고 메시지의 작업은 메시지 작성과 확인이다.

트랜잭션은 노드 간의 메시지 교환순서를 확인할 수 있다. 트랜잭션의 데이터 모델은 참여노드, 메시지 교환으로 구성되고 트랜잭션의 작업은 거래 개시, 거래 종료, 거래 확인이다.

전송은 다른 노드에 메시지를 보내는 적절한 수단을 제공한다. 전송의 구체적인 구현은 구현시 적합한 수단을 선택한다.

다음 그림은 노드, 메시지, 트랜잭션, 전송간의 관계와 프로세스를 보여준다.



(그림 39) 노드, 메시지, 트랜잭션, 전송간의 관계 및 프로세스

## 제 2 절 Trusted Web 서비스 설계

### 1. Trusted Web 서비스의 구현 요구사항

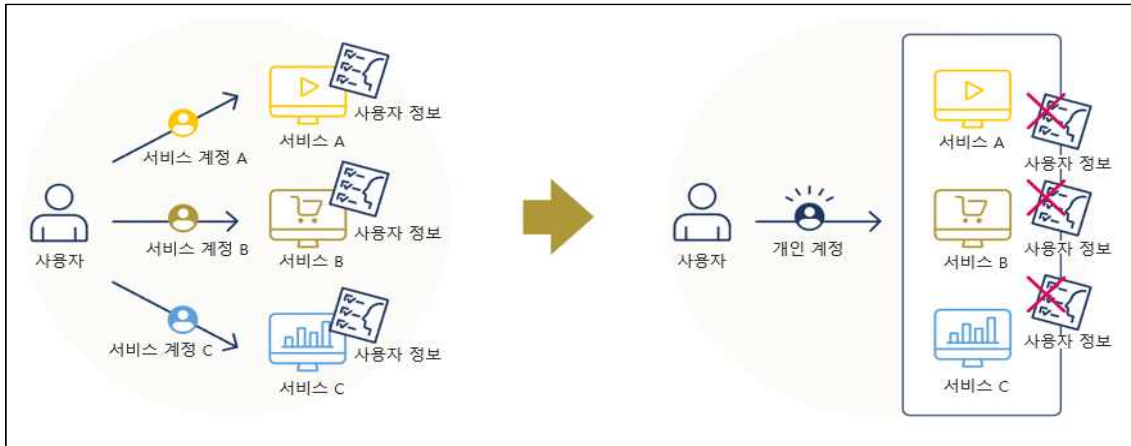
#### 1.1. 통합된 크리덴셜을 통한 다양한 서비스 접근

Trusted Web은 서비스마다 별도의 크리덴셜(계정)을 가지지 않으며, 하나의 통합된 크리덴셜을 사용하여 다양한 웹 서비스 및 플랫폼 서비스에 접근이 가능하다.

웹 서비스 제공자는 로그인시 필수 속성만 확인하면 되며, 고객의 개인정보를 보관할 필요가 없다. 이로 인해 유출위험 및 관리비용을 절감할 수 있다. 사용자는 자신의 검색 기록 및 웹 서비스 사용이 웹 서비스 제공자에게 알려지지 않도록 할 수 있으며 검색 기록을 기반으로 광고를 볼 가능성이 낮아지게 된다.

특정 서비스 계정에 의존하지 않고 사용자는 더 이상 여러 ID와 비밀번호를 관리할 필요가 없다. 사용자는 자신의 사용 데이터를 서비스 A에서 서비스 B로 연결하여 서비스 B와 사용 데이터를 공유하지 않고도 편리한 서비스를 받을 수 있다.

다음 그림은 통합된 크리덴셜을 통한 서비스 접근 구성도를 보여준다.



(그림 40) 통합 크리덴셜을 통한 다양한 서비스 접근 구성도

## 1.2. 개체 신뢰성

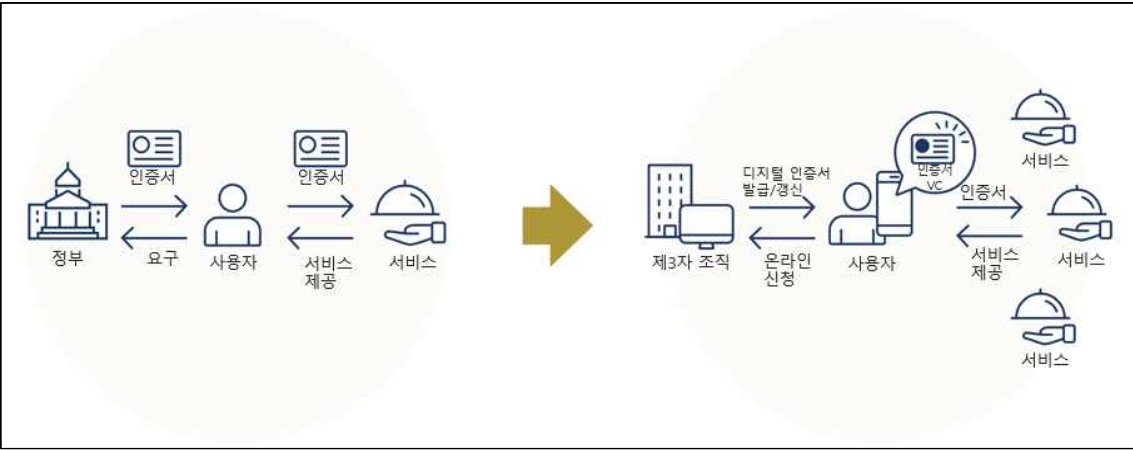
개체 신뢰성은 사용자의 디지털 신원을 증명·검증하는 과정이다. 이는 분산된 형태로 운영되는 Trusted Web에서 중요한 개념 중 하나로, 사용자가 자신의 데이터를 통제하면서도 다른 개체들과 안전하게 상호작용할 수 있는 프레임워크를 제공한다.

개체 신뢰성을 위한 신뢰된 신원증명의 주요 특징과 개념은 다음과 같다.

- o Self-Sovereign Identity(SSI): Trusted Web은 사용자에게 자체 주권신원을 제공한다. 사용자가 자신의 신원정보를 소유하고 통제할 수 있음을 의미한다.
- o Verifiable Credentials (VCs): Trusted Web은 사용자가 특정 주장(claim)에 대한 디지털 자격을 발행하고 검증할 수 있도록 한다. 이를 통해 사용자는 자신의 신원정보를 안전하게 제시하고 검증할 수 있다.
- o DID (Decentralized Identifier): Trusted Web은 분산원장에 저장된 고유한 식별자인 DID를 사용하여 사용자의 디지털 신원을 나타낸다. 이는 중앙 집중형 서버가 아닌 분산된 형태로 사용자의 정보를 관리한다.
- o DID Authentication: Trusted Web은 사용자가 DID를 사용하여 안전하게 로그인하고 시스템 또는 서비스에 대한 인증을 수행할 수 있는 방법을 제공한다.
- o 신뢰 수준 향상: Trusted Web은 검증 가능한 영역을 확대하여 사용자의 신뢰수준을 높이는 데 중점을 둔다. 이는 블록체인 등의 기술을 활용하여 합의 구축 및 데이터의 무결성을 보장한다.

다양한 주체가 쉽게 VC를 발행할 수 있기 때문에 사용자의 신뢰증명 비용과 서비

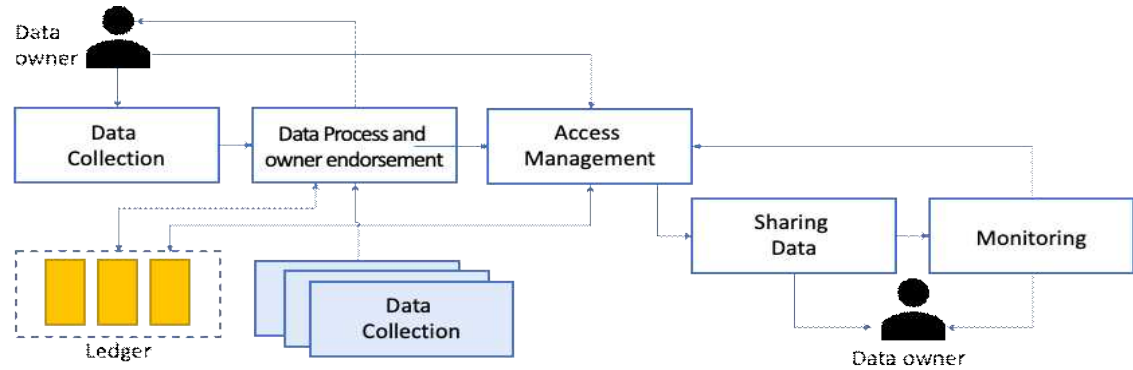
스 제공자의 검증 비용이 감소(표준화된 데이터 형식으로 인해 인증서의 유효성을 확인하기 위해 인증서를 수동으로 검사할 필요가 없으므로) 된다. 다양한 신뢰 증명은 “검증 가능한 크리덴셜”로 발행되며, 사용자는 이를 스마트폰이나 기타 장치의 지갑에 저장할 수 있다. 그런 다음 사용자는 이러한 자격 증명을 디지털 인증서로 사용하여 신뢰성을 입증할 수 있다. 다음 그림은 다양한 신뢰 증명 과정을 보여준다.



(그림 41) 다양한 신뢰증명 과정 예제

### 1.3. 데이터의 신뢰성

데이터의 신뢰성은 데이터의 정확성, 무결성, 안전성 및 보안성을 강화하기 위해 수행되는 전반적인 과정이다. 데이터의 신뢰성은 데이터의 출처, 변조 여부, 최신성 등을 확인하고 유지하는 과정에 중점을 둔다. 또한 데이터 자체에 대한 신뢰를 강화하고, 이를 통해 참여자들이 안전하게 데이터를 활용하고 확장할 수 있도록 지원한다. 다음 그림은 데이터 신뢰성을 위한 구성도를 보여준다.



(그림 42) 데이터 신뢰성을 위한 구성도

Trusted Web에서 데이터의 신뢰성을 강화하기 위해 사용되는 주요 특징과 기술은 분산원장 기술, 암호화 기술, 검증 가능한 데이터 교환 프로토콜, 데이터 품질 및 메타데이터 관리, 디지털 설명 및 인증, 분산형 아키텍처와 오버레이 접근법 등이 있다.

- 분산원장 기술: 분산원장 기술은 데이터의 변경 이력을 안전하게 기록하고 관리하는 데 중요한 역할을 한다. 분산된 네트워크에 분산된 데이터베이스를 제공하여 변경내역을 블록형태로 체인에 연결하여 안전한 기록을 제공한다.
- 암호화 기술: 데이터를 안전하게 전송하고 저장하기 위해 암호화 기술을 활용한다. 암호화는 데이터를 해독하기 어렵게 만들어 민감한 정보를 보호하고, 특히 데이터의 무결성을 보장하는 데 기여한다.
- 검증 가능한 데이터 교환 프로토콜: Trusted Web은 검증 가능한 데이터 교환을 위한 프로토콜을 통합한다. 이는 데이터 교환에 대한 합의를 구축하고 이를 추적하는 데 사용되며, 데이터의 정확성과 신뢰성을 제고한다.
- 데이터 품질 및 메타데이터 관리: 데이터 품질 및 메타 데이터 관리는 정확하고 신뢰성 있는 데이터를 유지하기 위한 핵심적인 요소이다. 데이터의 출처, 정확성, 최신성 등을 효과적으로 관리하여 데이터의 신뢰성을 높인다.
- 디지털 서명 및 인증: 디지털 서명과 인증 기술을 활용하여 데이터의 출처와 무결성을 보장한다. 이를 통해 데이터가 변조되지 않았음을 확인하고, 신뢰할 수 있는 출처에서 비롯된 것임을 검증한다.
- 분산형 아키텍처: 데이터를 분산된 형태로 관리하고 분산 아키텍처를 활용하여 중앙집중형 시스템의 단점을 극복한다.

#### [ 데이터 신뢰성과 제로 트러스트 비교 ]

데이터 신뢰성과 제로 트러스트(Zero Trust)는 모두 정보보안 및 신원관리에 관련된 컨셉이지만, 서로 다른 관점과 목표를 가지고 있다.

- **데이터 신뢰(Data Trust)**: 데이터 신뢰는 데이터의 정확성, 무결성, 안전성 및 신뢰성을 강화하기 위해 수행되는 전반적인 노력
- **제로 트러스트(Zero Trust)**: 전통적인 네트워크 보안 모델을 전환하여, 사용자나 기기가 네트워크 내에서 어디에 있든 상관없이 신뢰하지 않고 항상 검증하는 보안철학

데이터 신뢰성과 제로 트러스트는 상호 보완적으로 활용할 수 있다.

- 제로 트러스트 모델은 네트워크 안에서의 신뢰를 줄이고 검증을 강조하므로 데이터가 실제로 신뢰할 만한지에 대한 강력한 기준이 필요하다.
- 데이터 신뢰성을 강화하고 데이터의 무결성을 확보하는 노력은 제로 트러스트 모델 설계에 도움이 될 수 있다.
- 제로 트러스트 데이터에 접근하는 모든 시점에서의 신뢰성 검증이 강조되므로 악의적인 활동이나 데이터 변조를 사전에 방지할 수 있다.

#### 1.4. 거래 공정성

거래 공정성은 플랫폼과 참여자(이용자)간의 합의된 정책에 따라 투명하게 거래가 이루어져야 한다. 이를 위해서는 데이터에 대한 추적, 기록, 모니터링 등을 통해 데이터에 대한 투명성이 보장되어야 한다.

거래 공정성을 위한 주요 구성요소로는 스마트 컨트랙트, 데이터 추적과 분산저장 공간, 디지털 월렛과 데이터 관리 등으로 구성한다.

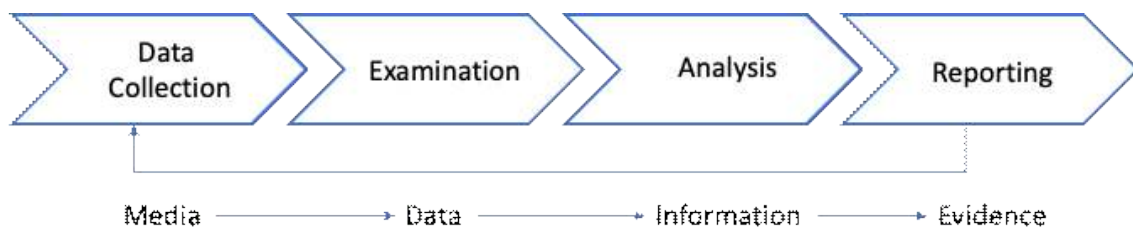
- o 스마트 컨트랙트: 거래의 조건과 규칙을 개체의 개입 없이 자동으로 거래하도록 한다. 거래 참여자 간의 합의를 프로그래밍적으로 정의하여 신속하고 투명한 거래를 보장한다. 스마트 컨트랙트의 실행결과는 안전한 분산 저장공간에 기록되어 변조없는 투명성을 제공한다.
- o 데이터 추적과 분산 저장공간: 거래 데이터는 안전한 분산 저장공간에 기록되어 데이터의 추적을 허용하고 분산 저장을 통해 신뢰성을 강화한다.
- o 디지털 월렛과 데이터 관리: 각 사용자는 통합된 크리덴셜을 이용해 신원정보 및 거래 데이터를 안전하게 디지털 월렛에서 관리한다. 디지털 월렛은 사용자 신원정보 및 거래기록을 안전하게 암호화하여 저장하고 관리한다. 사용자는 디지털 월렛을 통해 거래 참여와 데이터에 대한 통제권을 갖는다.

#### 1.5. 거래 추적성

데이터 추적은 데이터의 소스부터 변경과 소멸까지의 이력을 기록하고 모니터링하는 과정이다. Trusted Web에서는 데이터의 신뢰성과 거래 공정성을 위한 핵심 요소이다. 데이터 추적을 위한 주요 기술은 감사기록 및 분석, 시간적 추적, 규정준수 확인, 제3자 검증, 체인 오브 커스터디 등이 있다.

- o 감사기록(Audit): 거래 과정에서 발생한 모든 이벤트와 활동을 기록하고 정기적으로 검토한다. 거래발생, 수정, 삭제, 승인, 거부 등 다양한 활동을 포함한다.
- o 감사분석: 시스템 및 애플리케이션 단에서 발생한 감사기록 내용을 개체, 객체, 발생한 시간, 위치, 접근 값 등의 관점에서 검토하고 추적한다.
- o 시간적 추적: 거래의 발생 시점부터 변경 이력까지 시간적 흐름을 추적한다. 각 활동의 타임스탬프를 확인하여 개체를 식별하고 컴플라이언스에 따른 적절한 조치를 취할 수 있다.

- o 규정준수 확인: 거래와 관련된 규정(과금 정책, 개인정보 수집·이용 정책 등)을 준수하는지 확인한다. 감사는 규정준수에 대한 적합성을 평가하고 부적합성에 대한 사항을 식별한다.
- o 제3자 검증: 외부의 검증된 기관을 통해 거래의 추적성을 검증하고 확인하여 투명성을 확보한다.
- o 체인 오브 커스터디(Chain of Custody): 데이터 이동과 변경 발생시 전자적으로 기록하고, 일치성을 검토하는 과정이다. 데이터의 신뢰성과 무결성을 강화하며, 변조시 추적이 가능하다. 다음은 Chain of Custody의 동작 예제를 보여준다.



(그림 43) Chain of Custody 예제

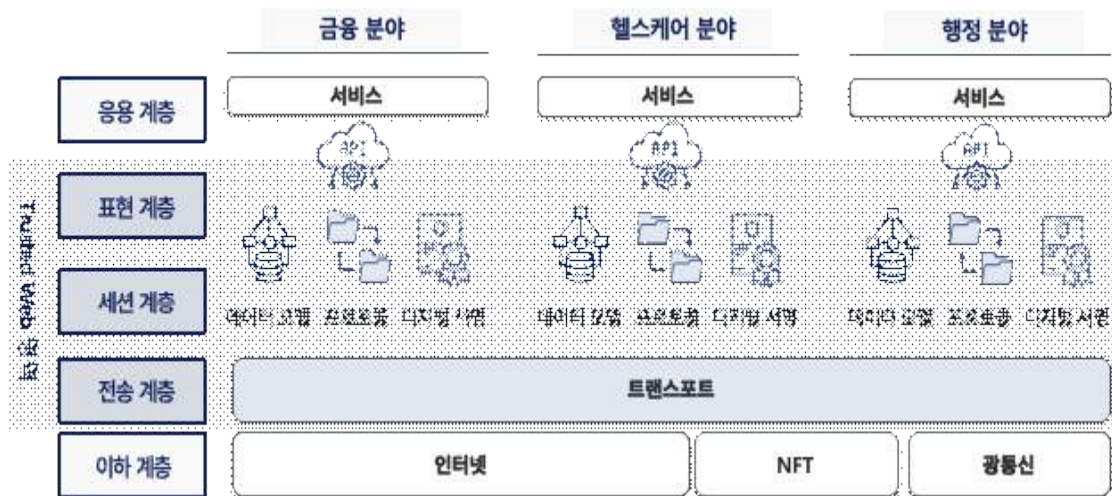
#### 1.6. 구축 기법: 오버레이 접근법

Trusted Web은 실현을 위한 로드맵으로 오버레이 접근법을 사용한다. Trusted Web의 아키텍처는 프레임워크를 구현하기 위한 기술적 기반으로, 네트워크 프로토콜 아키텍처 계층 모델로 설명할 수 있다.

물리적 계층을 바탕으로 전송계층과 세션계층, 표현계층, 응용계층 등의 개별 서비스 계층 사이에서 미들웨어 형태로 구성한다. 미들웨어에서는 호환 가능한 API, 데이터 모델 및 프로토콜이 식별되어 상호 운용성을 보장하고 표준화를 이끌어 낸다. Trusted Web은 각 분야의 인프라로 형성되고 다양한 서비스를 통해 피드백을 받아 실현될 수 있다.

다음 그림은 오버레이 접근법을 도식화 한 것이다.





(그림 44) Trusted Web 아키텍처 모델

## 2. Trusted Web 서비스 설계 원칙

국가별 Trusted Web 관련 구축 및 활용 현황을 분석한 결과, 아직까지는 중앙화 플랫폼에 의존적으로 개인정보 주권 및 데이터 주권에 한계가 있으며, 다양한 개인속성 값 활용 한계로 인해 정부에서 제공하는 서비스에 국한되어 서비스가 제공되고 있다. 따라서, 플랫폼 서비스에 대한 투명성과 공정성 문제는 여전히 문제로 남아 있다.

앞서 살펴본 현 인터넷/웹의 문제점을 해결하기 위해 Trusted Web에 대한 정의와 설계원칙을 다음과 같이 설정한다.

### 2.1. Trusted Web의 정의

**” 現 인터넷의 문제점을 해결하고 안전한 정보공유와 디지털 창작물의 공정한 거래가 가능한 인터넷 환경 ”**

Trusted Web은 아래의 4가지 항목을 만족한다.

- o 신뢰된 사용자(Trusted User)
- o 신뢰된 데이터(Trusted Data)
- o 신뢰된 취급자(Trusted Data Processor)
- o 공정한 플랫폼(Trusted Platform)



## 2.2. Trusted Web의 설계원칙

Trusted Web 설계원칙은 다음과 같이, 자기주권, 신뢰통신, 데이터 추적, 독립성, 분산화로 구성된다.

### 2.2.1. 자기주권

자기주권은 사용자(개인 또는 조직)가 자신의 개인정보와 디지털 창작물에 대한 완전한 관리권한을 가지는 개념이다. 이는 사용자가 자신의 데이터를 효과적으로 소유하고, 데이터에 대한 접근 및 이용에 대한 주도권을 소유함을 의미한다. 자기주권은 디지털 환경에서 개인의 권리와 개인정보 보호를 강화하며, 사용자 중심의 데이터 관리를 지원한다.

### 2.2.2. 신뢰통신

신뢰통신은 데이터의 진본성을 검증하고, 전송 데이터의 무결성과 비밀성을 보장하는 기술 및 프로세스를 나타낸다. 이는 디지털 통신에서 데이터가 송수신 과정에서 변조되지 않고 안전하게 전송되도록 하는 것을 목표로 한다. 따라서 신뢰통신은 믿을 수 있는 통신채널을 확립하고 데이터의 안전한 교환을 지원하여 디지털 환경에서의 신뢰성을 강화한다.

### 2.2.3. 데이터 추적

데이터 추적은 사용자의 데이터에 누가 언제, 어떻게 접근했는지를 정확하게 기록하고 모니터링하는 과정이다. 이는 사용자가 자신의 데이터에 대한 투명성을 확보하고, 데이터의 이력을 추적하여 무단접근이나 변경을 감지하는데 핵심기능이다. 데이터 추적은 보안 및 규정준수를 강화하며, 플랫폼 서비스 사업자와의 거래 공정성을 보장하고, 사용자에게 데이터 이용에 대한 강력한 통제를 제공한다.

### 2.2.4. 독립성

독립성은 특정 서비스나 플랫폼에 지나치게 의존하지 않는 원칙이다. 사용자는 다양한 서비스 및 플랫폼 간에 유연하게 이동하고, 자신의 데이터를 특정 생태계에 고정되지 않고 관리할 수 있어야 한다. 독립성은 사용자의 서비스 및 플랫폼에 대한 선택의 폭을 확장하고, 플랫폼 서비스 사업자와의 거래 공정성을 이끌어 낼 수 있으며, 개인의 디지털 경험을 다양화하는 데 기여한다.

## 2.2.5. 분산화

분산화는 분산 스토리지 및 지갑을 활용하여 데이터를 중앙화된 위치가 아닌 여러 위치에 저장하고 관리하는 원칙이다. 이는 데이터의 신뢰성을 강화하고, 분산된 환경에서의 안전한 데이터 관리를 지원한다. 분산화는 단일 장애 지점을 피하고 데이터의 안전성을 향상함으로써 보안 및 안전성 측면에서 중요한 역할을 한다.

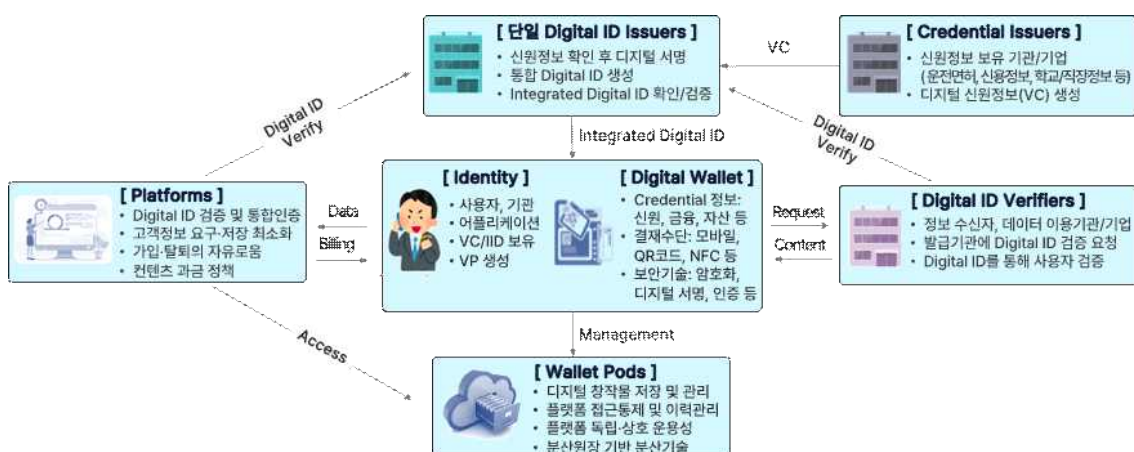
### [ Trusted Web의 설계원칙 ]

- **자기주권**: 사용자(개인, 조직)는 자신의 개인정보와 디지털 창작물에 대한 관리 권한을 가진다.
- **신뢰통신**: 데이터의 진본성을 검증하고, 전송 데이터의 무결성과 비밀성을 보장한다.
- **데이터 추적**: 사용자의 데이터에 언제 누가 접근했는지를 추적한다.
- **독립성**: 특정 서비스 및 플랫폼에 과도하게 의존하지 않는다.
- **분산화**: 분산 스토리지 및 지갑을 사용하여 데이터 분산관리를 한다.

## 3. Trusted Web 서비스 구성요소

Trusted Web 서비스 구성요소는 Trusted Web 설계원칙을 만족하기 위한 객체들로 구성한다. Trusted Web 서비스 구성요소의 가장 큰 특이점은 공공 및 민간 서비스를 포함하며 모든 플랫폼에서 동일하게 사용할 수 있는 단일 Digital ID를 생성하는 기관을 추가한다. 또한, 개인의 Digital Wallet과 연결하여 사용자의 모든 디지털 데이터를 저장하고 접근기록을 관리하는 Wallet Pod 개념을 적용한다.

다음 그림은 Trusted Web의 서비스 구성요소를 보여준다.



(그림 45) Trusted Web 서비스 구성요소

### 3.1. Identity

Identity는 참여자로 이용자, 기관, 애플리케이션이 될 수 있다. Identity는 신뢰된 디바이스에 Digital Wallet을 생성하여 VC, 통합 ID(IID, Integrated ID), VP를 저장하고 관리한다. Identity는 VC를 기반으로 단일 Digital ID Issuer로부터 IID를 발급받아 관리하며, VC로부터 VP를 생성하여 서비스 사용기관(Platform, Digital ID Verification)에 따라 적절한 VP 값을 제공한다.

### 3.2. Digital Wallet

Digital Wallet은 Credential 정보를 통해 신원, 금융, 자산 등을 관리한다. 안전한 데이터 거래 및 금융거래를 위해 암호화, 디지털 서명, 인증과 같은 보안기술을 활용하며, 결제방법으로 모바일, QR코드, NFC 등 다양한 수단을 사용한다.

### 3.3. Digital ID Verifier

Digital ID Verifier는 정보를 수신하는 정보 수신자, 데이터 이용기관, 플랫폼 서비스 및 사업자 등이다. Digital ID Verifier는 단일 Digital ID Issuer를 통해 Identity의 Digital ID를 검증한다.

### 3.4. 단일 Digital ID Issuer

단일 Digital ID Issuer는 Identity에게 IID를 발급해 주는 기관이다. 단일 Digital ID Issuer는 IID 발급을 위해 Credential Issuer를 통해 Identity의 VC로 신원을 검증한다. 신원이 검증되면 Identity에게 IID를 발급한다.

### 3.5. Credential Issuer

Credential Issuer는 Identity의 신원정보를 보유한 기관 또는 기업이다. 신원정보는 운전면허 정보, 신용정보, 학교정보, 직장정보 등이다. Credential Issuer는 Identity의 VC를 검증하며, Identity의 신원정보를 안전하게 관리한다.

### 3.6. Platform

Platform은 마켓플레이스, 지불, SNS, 저장소, 검색엔진 등 서비스 사업자가 해당된다. Identity가 서비스 이용시 Digital ID에 대한 검증요청을 하고, 신뢰된 Identity에게 서비스를 허용한다. 또한, Identity가 소장한 디지털 정보 또는 개인정보를 활용하기 위해 Wallet Pods에 접근하며, 이때도 Identity의 Digital ID를 검증요청하여 신뢰된 사용자인지를 확인한다.

Platform은 Identity에 대한 개인정보 수집과 저장을 최소화하고, 가입과 탈퇴가 자유로워야 한다. 또한, identity가 생성한 디지털 창작물에 대한 이용에 대해 과금정책을 공유하고, 과금정책에 따라 Identity와 공정하고 투명한 배분을 집행한다.

다음은 현재 활동중인 인터넷 Platform 분류와 사업자를 보여준다.



(그림 46) 인터넷 Platform 서비스 사업자

### 3.7. Wallet Pod

Wallet Pod는 Digital Wallet의 정보를 백업하고 Identity의 디지털 창작물에 대한 저장과 관리를 수행하는 분산화된 저장공간 서비스이다. Wallet Pod은 Identity가 수행하는 모든 행위(서비스 접근, 이용, 종료 등)를 기록하고 관리한다.

Wallet Pod 서비스 사업자는 Identity의 독립성과 상호 운용성을 보장하며, 분산원장 기반 분산기술을 통해 Identity의 데이터를 안전하게 보관한다.

## 4. Trusted Web 서비스 주요 기능 및 설계

Trusted Web을 구성항목인 신뢰된 사용자, 신뢰된 데이터, 신뢰된 취급자, 공정한 플랫폼을 만족하기 위해 다음과 같이 4개의 기능을 구현한다.

- 통합 ID 생성 및 관리(분산화)
- 신뢰통신(데이터 진본성)
- 동적동의(자기주권)
- 데이터 추적(공정성, 독립성)



(그림 47) Trusted Web의 4가지 핵심기능

### 3.1. 통합 ID 생성 및 관리(분산화)

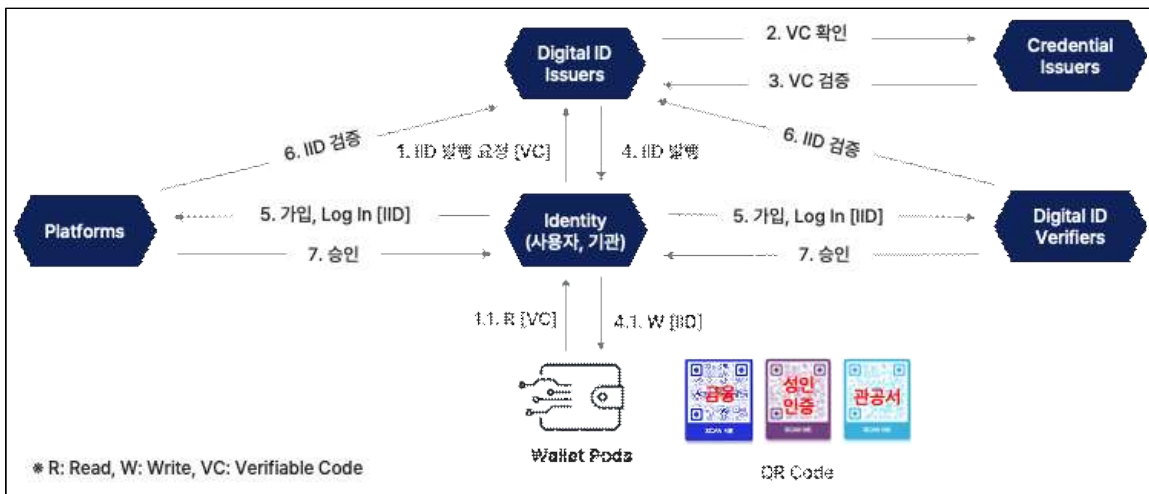
통합 ID는 공공기관 및 민간 서비스 플랫폼 등 인터넷상에서 공통으로 사용할 수 있는 ID이며, 현실의 Identity를 유일하게 증명하는 수단이다.

사용자는 크리덴셜을 통해 통합 IID를 발행하고, DID(Decentralized ID)에 연계한다. IID는 객체와 연결된 유일한 인증정보로, 다양한 온라인 플랫폼에서 고유한 신원으로 인증한다. VC(Verifiable Code)를 QR코드로 변환하여 오프라인 서비스(예: 차량렌트, 신분조회 등)에서 신상정보(생년월일, 주민번호 등)노출 없이 인증할 수 있다.

통합 ID 생성과정은 다음과 같다.

- ① Identity는 Wallet Pod에 있는 VC를 추출하여 Digital ID Issuer에게 IID 발급을 요청한다.
- ② Digital ID Issuer는 Identity의 VC를 보유한 Credential Issuer에 VC 검증을 요청한다.
- ③ Credential Issuer는 Identity의 VC를 검증하고 검증결과를 Digital ID Issuer에게 통보한다.
- ④ Digital ID Issuer는 검증된 VC를 이용해 IID를 생성하여 Identity에 전달한다. Identity는 발급받은 IID를 자신의 Digital Wallet에 저장하고, Wallet Pod에 백업한다. Wallet Pod은 IID를 저장하고, 데이터 추적을 위한 감사기록을 남긴다.
- ⑤ Identity는 서비스 기관(Digital ID Verifier, Platform)에 IID를 이용하여 가입 또는 데이터 접근 등을 시도한다.
- ⑥ 서비스 기관은 Identity의 IID를 Digital ID Issuer를 통해 검증하여 신뢰된 사용자인지를 확인한다.
- ⑦ 서비스 기관은 신뢰된 사용자에 대해 가입 또는 서비스 사용을 허가한다.

다음 그림은 통합 ID 생성과정을 보여준다.



(그림 48) 통합 ID 생성 과정

### 3.2. 신뢰통신(데이터 진본성)

Identity는 납세증명서, 건축대장, 건강보험 관련 정보 등과 같은 디지털 콘텐츠 발행 요청 시 안전하게 전달하기 위해 디지털 서명 및 암호화를 수행한다. 이를 통해 Identity는 자신의 데이터를 안전하게 유지하면서 필요한 정보를 공유할 수 있다.

플랫폼은 Identity가 저장한 디지털 콘텐츠에 접근할 때도 디지털 서명 및 암호화를 수행하여 데이터의 안전성을 유지하고, 무단 접근을 방지한다.

Wallet Pod은 플랫폼 접근 이력을 포함해 Identity의 모든 활동을 기록하고 관리함으로써 사용자에게 보다 투명하고 안전한 디지털 경험을 제공한다.

신뢰통신을 설명하기 위해 Identity의 디지털 콘텐츠에 대한 요청과 플랫폼의 Wallet Pod에 대한 접근과정을 예로 든다.

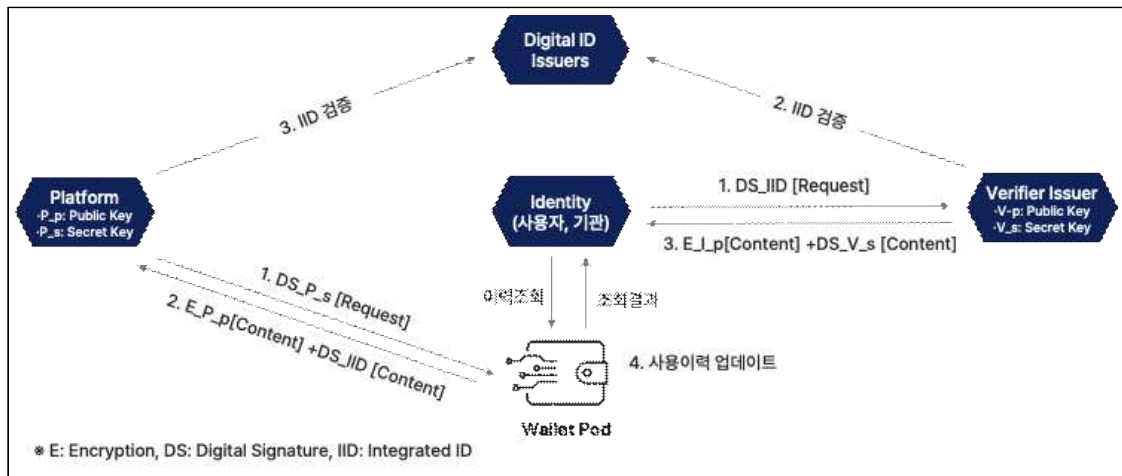
Identity의 디지털 콘텐츠에 대한 요청과정에 대한 신뢰통신 과정은 다음과 같다.

- ① Identity는 Verifier Issuer에게 Request 내용을 자신의 IID(Secret Key)로 서명하여 전달
- ② Verifier Issuer는 IID를 Digital ID Issuer를 통해 검증하고 신뢰된 Identity임을 확인
- ③ Verifier Issuer는 IID의 공개키(I\_p)로 디지털 콘텐츠를 암호화하고, 자신의 비밀키(V\_s)로 디지털 서명하여 Identity에 전송
- ④ Wallet Pod은 Identity의 모든 거래 내용을 기록하며, Identity는 언제든지 거래 내용에 대한 이력조회를 통해 관리

플랫폼의 Wallet Pod에 대한 접근과정에 대한 신뢰통신 과정은 다음과 같다.

- ① Platform은 Wallet Pod에게 Request 내용을 자신의 비밀키(P\_s)로 디지털 서명하여 전달
- ② Wallet Pod은 Platform의 요청을 수용하고, 디지털 콘텐츠를 Platform의 공개키(P\_p)로 암호화하고, Identity의 IID로 서명하여 전달
- ③ Platform은 Identity가 신뢰된 사용자인지를 확인하기 위해 Digital ID Issuer에게 IID 검증 요청
- ④ Wallet Pod은 Platform의 모든 접근이력을 기록하며, Identity는 언제든지 거래 내용에 대한 이력조회를 통해 관리





(그림 49) 신뢰통신 과정

### 3.3. 동적동의(자기주권)

동적동의는 사용자가 개인정보 처리에 대한 동의를 제어하는 개념으로 사용자가 언제든지 동의를 철회하거나 변경할 수 있는 방식으로 구현되어야 한다. 동적동의는 사용자에게 수집 및 처리의 목적, 범위, 기간 등을 더 세부적으로 제어할 수 있는 기능을 제공한다. 이를 통해 사용자에게 투명하고 개인화된 데이터 관리를 허용하며, 사용자의 우선권과 프라이버시를 존중하는 원칙을 제공한다. Identity는 개인정보 제공의 편의성을 위해 VP Policy를 생성하여 관리한다. VP Policy는 개인의 다양한 속성정보를 제공처의 이용 목적과 기간에 따라 그룹을 생성한 것이다.

다음 그림은 VP Policy를 생성하는 예를 보여준다.

기본정보	이름	성별	생년월일	...
연락처	주소	전화번호	이메일	...
바이오	지문	홍채	얼굴	...
건강정보	의료기록	혈액형	알러지	...
금융정보	은행계좌	주식보유	신용카드	...
교육·직업	학교·학점	직장·성과	학습이력	...
인터넷활동	쇼핑정보	검색기록	SNS	...
VP Policy A:	기본정보	연락처	알러지	Time
VP Policy B:	바이오	금융정보	쇼핑정보	Time

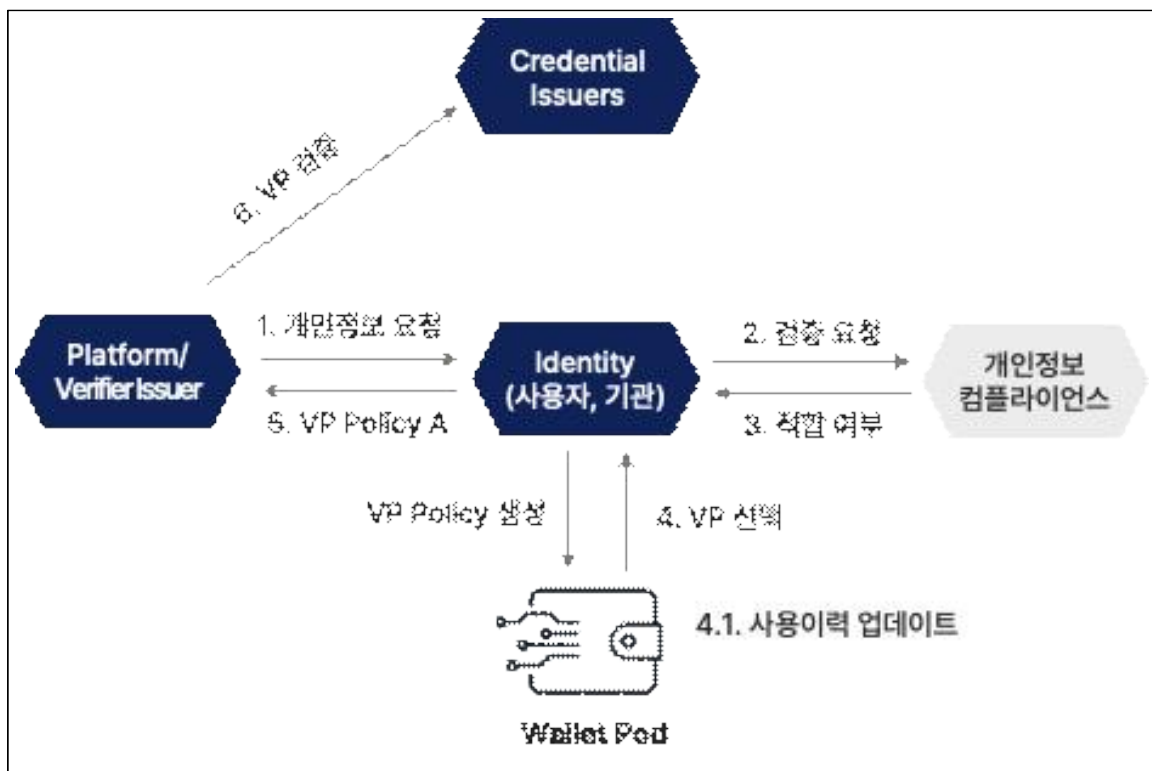
(그림 50) VP(Verifiable Presentation) Policy 생성 예



동적동의를 위한 과정은 다음과 같다.

- ① Platform 또는 Verifier Issuer는 Identity에게 개인정보를 요청
- ② Identity는 자체적으로 요청된 개인정보 수집 목적과 범위, 기간을 검토하여 VP를 제공하거나 개인정보 컨플라이언스 점검도구를 활용해 검증을 요청
- ③ 개인정보 컨플라이언스 도구는 개인정보를 수집 및 이용하려는 기관의 서비스 범위와 목적에 따라 개인정보 수집범위를 판단해 주는 서비스 도구로 Identity의 검증요청을 판단하여 결과 통보
- ④ Identity는 개인정보 컨플라이언스 도구의 판단에 따라, 적합한 VP를 Wallet Pod에서 선택. Wallet Pod은 모든 접근내용을 기록
- ⑤ Identity는 적합한 VP Policy를 Platform 또는 Verifier Issuer에게 제공
- ⑥ Platform 또는 Verifier Issuer는 제공받은 VP 내용을 소장한 Credential Issuer를 통해 검증

다음 그림은 동적동의 절차를 보여준다.



(그림 51) 동적동의 과정

### 3.4. 데이터 추적(공정성, 독립성)

데이터 추적성은 데이터의 이동과 사용에 대한 정확한 기록을 저장하고 관리함으로써 모든 거래의 투명성을 제공하는 것이 목적이다. 데이터 추적성을 통해 플랫폼과의 거래 공정성을 확보하고, 특정 플랫폼에 종속성을 탈피할 수 있다.

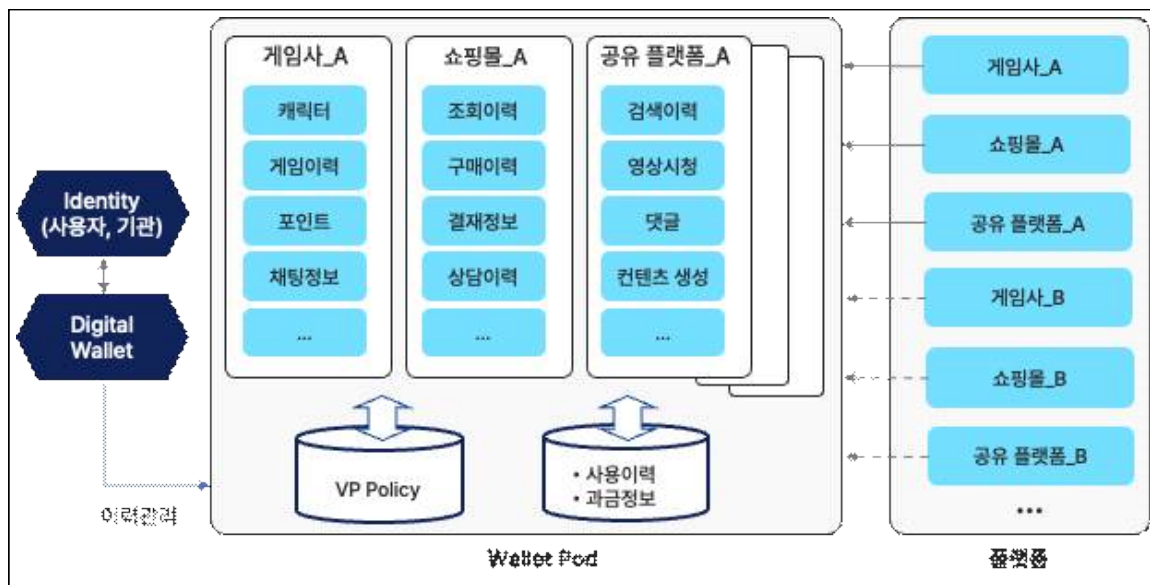
Identity는 Wallet Pod 서비스 제공자를 선택하고, 모든 인터넷 활동에 대한 기록을 안전하게 저장하고 관리한다. 이를 통해 사용자는 디지털 활동과 관련된 데이터를 분산환경에서 효과적으로 관리할 수 있다.

Identity는 선택한 플랫폼에서 제공하는 다양한 서비스와 과금정책에 따라, 자신에게 가장 유리한 플랫폼을 선택하고 해당 플랫폼에 가입하여 활동한다. 이 과정에서 사용자는 플랫폼과의 상호작용을 통해 자신의 정보를 제공하게 된다.

플랫폼이 Identity의 디지털 창작물에 대한 접근 또는 Identity의 플랫폼 활동정보를 사용하려 하는 경우, Wallet Pod은 모든 이력정보를 기록하고 관리한다. 모든 접근 또는 사용이력에 따라, 플랫폼은 Identity에게 과금정책에 따라 투명하게 Identity에게 과금을 지불한다.

사용자는 데이터 추적을 통해 자신의 활동과 관련된 정보들 통제하며, 플랫폼과의 상호작용에서 공정한 거래를 수행하고 독립성을 보장받는다.

다음 그림은 데이터 추적에 관한 개념을 보여준다.



(그림 52) 데이터 추적 개념도

#### 4. 현안 및 향후 고려사항

Trusted Web이 해결해야 할 문제는 첫 번째로 데이터가 보관된 장소에 구애받지 않고 데이터 자체를 검증할 수 있어야 한다. 두 번째로 데이터가 보관될 수 있는 위치 간의 데이터 관련 상호작용을 확인할 수 있어야 한다. 따라서 기존 기술을 최대한 재사용하고 결합 가능한 기술을 파악 정리하여 새로운 기술을 개발할 필요가 있다. 마지막으로 공통 ID를 개발하고 활용하는 문제는 정부의 정책(거버넌스)개발과 이해관계자들간의 충분한 논의와 협의가 이루어져야 한다.

한국의 정보통신 서비스와 현황에 따른 한국형 Trusted Web을 구축하기 위해서는 다음과 같은 추가적인 검증과 투자가 필요하다.

##### 4.1. Trusted Web 주요 기능에 대한 세부 절차 설계 및 검증

앞서 Trusted Web에 대한 주요 기능을 정의하고 서비스 설계를 진행했으나, 서비스를 구현하기 위한 세부절차와 기술에 대한 논의가 부족하다. 또한, 한국의 정보통신 서비스와 구현환경을 고려하여 적합한 기술을 개발 또는 선택하며, 검증하는 절차가 필요하다.

##### 4.2. Trusted Web 프로토타입 설계 및 구현을 통해 현실적인 문제점을 도출

각 국가는 Trusted Web에 대한 개념을 정립하고, 이를 구현하기 위해 다양한 Use Case를 개발하고 문제점들을 도출하고 있으며, 도출된 문제점들을 보완하는 과정을 통해 성숙된 모델을 개발해 나가고 있다.

따라서, 한국형 Trusted Web을 구축하기 위해서는 다양한 Use Case를 구상하고 시범적으로 운영을 통해 문제점을 극복해 나가는 과정이 필요하다.

## [참고문헌]

- [1] Trusted Web 推進協議会, “Trusted Web ホワイトペーパー Ver2.0 ”, 2022.
- [2] Trusted Web 推進協議会, “Trusted Web white paper ver. 2.0 executive summary”, 2022.
- [3] NTT Data, “Trusted Web 共同開発支援事業に係る調査研究”, 2023.
- [4] 株式会社エヌ・ティ・ティ・データ経営研究所, “令和4年度デジタル取引環境整備事業  
（「Trusted Web」の実現に向けた技術動向調査”, 2023.
- [5] Andrei Vlad Sambra, “Solid: A Platform for Decentralized Social Applications Based on Linked Data”, 2016.
- [6] Essam Mansour, “Trusted Web White A Demonstration of the Solid Platform for Social Web Applications”, 2016.
- [7] European Commission, “European Digital Identity Architecture and Reference Framework - Outline -”, 2022.
- [8] IDunion, “Empowering Sustainable Products and Consumer Confidence through Verifiable Credentials - A Case Study on Digital Product Passport with GS1 Standards Whitepaper“, 2023.
- [9] The United Kingdom Government, “UK digital identity & attributes trust framework alpha v2 (0.2)”, 2023.
- [10] NIST, “SP800-63-3 Digital Identity Guidelines”, 2020.
- [11] NIST, “SP800-63A Enrollment and Identity Proofing”, 2020.
- [12] NIST, “SP800-63B Authentication and Lifecycle Management”, 2020.
- [13] NIST, “SP800-63C Federation and Assertions”, 2020.
- [14] DIACC, “PCTF Digital Wallet Component Overview”, 2023.
- [15] Australian Government, “Trusted Digital Identity Framework Release 4.8”, 2023.
- [16] 한국저작권위원회, “웹3.0 산업현황 보고서”, 2023.
- [17] 윤영진, 황재진, “웹3.0과 메타버스가 만드는 디지털 혁명”, 제이펍, 2023.
- [18] ETRI 블록체인기술연구센터, 윤대근, “자기주권 신원증명 구조 분석서”, 제이펍, 2020.
- [19] Trusted Web website, “About Trusted Web Page”, <https://trustedweb.go.jp/en/about/>
- [20] Trusted Web website, “Use Cases”, <https://trustedweb.go.jp/en/use-cases/>
- [21] Trusted Web website, “White Papers · Related Materials”, <https://trustedweb.go.jp/en/documents/>
- [22] Trusted Web website, “Public Offering for Use Cases”, <https://trustedweb.go.jp/en/public-offering/>
- [23] NTT Data, “「Trusted Web の実現に向けたユースケース実証事業」公募実施のお知らせ

- せ”, [https://www.nttddata-strategy.com/newsrelease/news/trusted\\_\\_web3\\_koubo/](https://www.nttddata-strategy.com/newsrelease/news/trusted__web3_koubo/)
- [24] TOPPAN SOCIAL INNOVATION, “令和4年度補正 Trusted Web の実現に向けたユースケース実証事業」に関するお知らせ”, [https://www.toppan.com/ja/joho/social/trusted\\_web2023\\_koubo.html](https://www.toppan.com/ja/joho/social/trusted_web2023_koubo.html)
- [25] Solid Project website, “Solid Project”, <https://solidproject.org/>
- [26] European Commission website, “European Digital Identity Architecture and Reference Framework - Outline”, <https://digital-strategy.ec.europa.eu/en/library/european-digital-identity-architecture-and-reference-framework-outline>
- [27] IDunion website, “About the project”, <https://idunion.org/projekt/?lang=en>
- [28] The United Kingdom Government website, “Cyber Security Documents”, <https://www.gov.uk/government/publications/uk-digital-identity-attributes-trust-framework-updated-version>
- [29] NIST website, “Digital Identity Guidelines”, <https://pages.nist.gov/800-63-3/>
- [30] DIACC website, “Trust Framework”, <https://diacc.ca/trust-framework/>
- [31] DIACC website, “Pan-Canadian Trust Framework<sup>TM</sup> Digital Wallet”, <https://diacc.ca/trust-framework-components/pctf-digital-wallet/>
- [32] Australian Government website, “Trusted Digital Identity Framework (TDIF)”, <https://www.digitalidentity.gov.au/tdif>
- [33] New Zealand Government website, “Digital Identity Services Trust Framework”, <https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/trust-framework/>
- [34] Medium website, “STACK-X Webinar – National Digital Identity Stack: Introduction to NDI”, <https://medium.com/ndi-sg/stack-x-webinar-national-digital-identity-stack-introduction-to-ndi-34b5dbed9565>
- [35] IndiaStack website, “India Stack is”, <https://indiastack.org/>
- [36] Nostr website, “A decentralized social network with a chance of working”, <https://nostr.com/>
- [37] Damus website, “The social network you control”, <https://damus.io/>
- [38] 한국데이터산업진흥원(Kdata), “마이데이터”, [https://www.kdata.or.kr/kr/contents/mydata\\_01/view.do](https://www.kdata.or.kr/kr/contents/mydata_01/view.do)
- [39] 개인정보보호위원회, “개인정보포털”, <https://www.privacy.go.kr/front/main/main.do>
- [40] Economic Forum, “Earning Digital Trust:Decision-Making forTrustworthy Technologies” , Insight Report, 2022.11

## <첨부 1> 일본: Trusted Web Use Case 분석

### 1. 2022년 「Trusted Web의 실현을 위한 유스 케이스 실증 사업」 공모 채택 결과

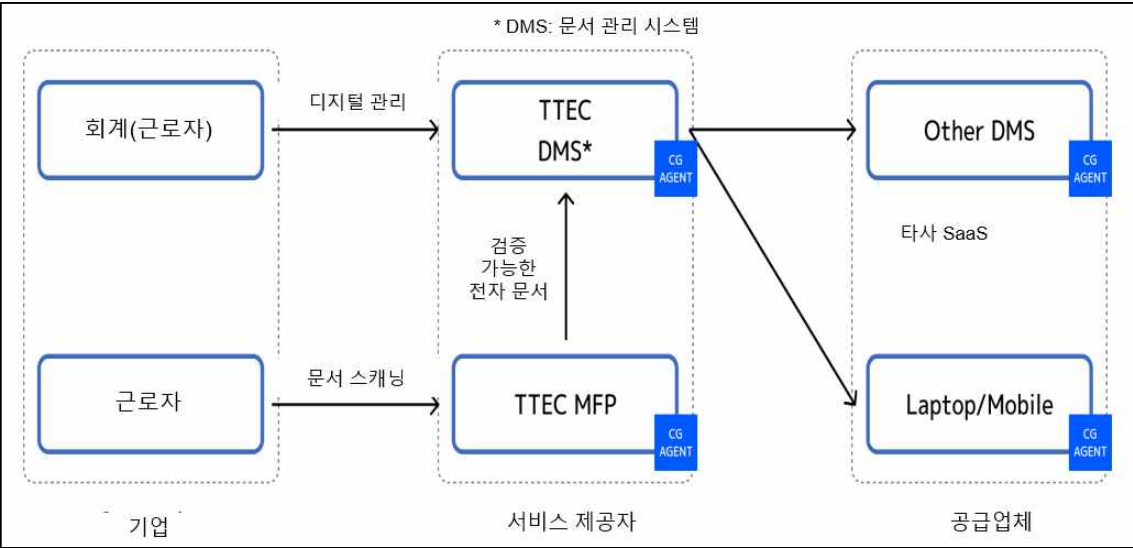
No.	사업자명 · 컨소시엄명	대표단체명 (컨소시엄의 경우)	유스 케이스 개요
1	Trusted Workplace Solution by TTEC and CG	도시바테크	작업장의 신뢰할 수 있는 전자화 문서 유통 시스템
2	ORPHE	—	하지 운동기 질환 환자와 의사, 연구자 간 신용할 수 있는 보행 데이터 유통 시스템
3	인재육성을 위한 Trusted 학수정보 유통시스템 개발 컨소시엄	후지쯔 Japan	인적 자원 육성을 위한 신뢰할 수 있는 교육 정보 유통 시스템
4	DataGateway PTE LTD	—	분산형 ID를 활용한 탄소 배출량 추적 시스템
5	SSI/FIDO 컨소시엄	도쿄대학	학수력 등의 본인 관리에 의한 인재 유동의 촉진
6	안마 홀딩스	—	기계 제품 공급망의 추적성 관리
7	DataSign	—	온라인 마케팅에서 개인 데이터 유통
8	덴츠 · ISID 퍼블릭 DX 컨소시엄	덴츠	중소법인·개인 사업자를 대상으로 하는 보조금·급부금의 전자 신청에 있어서의 “본인 확인·실재 증명”의 새로운 구조
9	산업회 증명서 디지털화 컨소시엄	정보서비스산업협회	법인세제와 공업회 증명서
10	헬스케어 정보 유통 시스템 개발 컨소시엄	시믹	임상 시험 및 의료 현장에서 신뢰성과 응용 가능성이 높은 정보 유통 시스템
11	알렉사라 네트워크	—	Trusted Network를 통한 사회 IT 인프라의 신뢰성과 강인성 향상 실현
12	대일본 인쇄	—	공동 앱에서 플랫폼을 넘어 사용자 트러스트 공유
13	메타버스×자기주권형 ID컨소시엄	NRI 디지털	가상 현실 공간에서의 서비스 이용 자격과 제공 데이터의 Trust 검증

※ 출처: NTT 데이터 경영연구소([https://www.nttdata-strategy.com/newsrelease/\\_news/trusted\\_\\_webr3\\_koubo/](https://www.nttdata-strategy.com/newsrelease/_news/trusted__webr3_koubo/))

2022-1. 도시바테크 (신뢰할 수 있는 업무용 디지털문서 유통 시스템)

【유스케이스 구성도】

- ① 국제 SDO인 W3C의 DID 및 VC 표준을 활용하여 MFP에서 생성된 감사 추적을 통해 문서를 디지털화하고 배포할 수 있다.
- ② 특정 산업 및 운영 분야의 서류 작업을 디지털화하여 작업자 생산성을 높이고 백 오피스 비용을 줄이며 작업 스타일을 개선할 수 있다.
- ③ CG의 데이터 인프라 솔루션을 사용하면 저렴한 비용으로 MFP 장치와 클라우드 간에 검증 가능한 전자 문서 교환을 구축할 수 있다.



【검증해야할 데이터】

- 언제, 누구에 의해, 어떤 MFP 장치에서 생성되었는지 확인하기 위한 디지털 문서이다.
- MFP 식별자(DID), 사용자 이름 및 일련 번호는 메타 데이터로 사용된다.
- MFP는 검증 가능한 자격 증명을 생성하여 DIDComm 암호화 메시지로 문서 관리 시스템에 보낸다.

검증 필요 문제	검증 대상	검증 방법	검증자
디지털 문서의 감사 재판	디지털 문서 인증	VC 서명 검증	문서 관리 시스템

【합의 구축과 추적】

MFP를 소유하거나 사용하는 최종 사용자는 서비스 제공업체와의 서비스 조건에 동의

한다. 최종 사용자는 서비스 제공자에게 트래픽 로그 확인을 요청하여 합의된 조건이 충족되고 있는지 확인할 수 있다. 트래픽 로그는 CG의 HUB((주)콜라보게이트에 의해 에이전트간 암호화된 데이터를 중계하는 중계서버)에 저장되며, 언제, 어떤 기기(식별자) 데이터가 어느 목적지로 전송되었는지 확인할 수 있다.

**【실현 내용】**

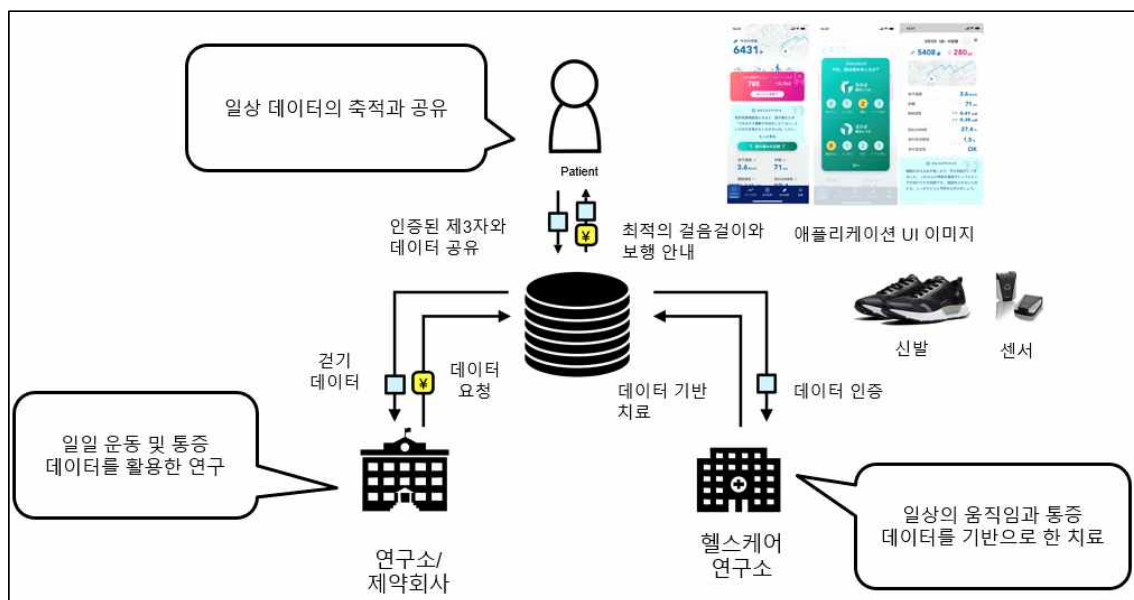
- 기존 MFP의 사용자 경험을 바꾸지 않고도 감사 추적이 필요한 문서를 누구나 쉽게 디지털화할수 있음을 확인하였다.
- 상기 목적을 달성하기 위한 신뢰할 수 있는 데이터 인프라를 저비용으로 구축할 수 있음을 확인한다(데이터 인프라를 처음부터 구축하는 것에 비해 약 30억원의 비용 절감(당사 계산 기준)).
- 다양한 장치에 유사한 인프라를 배포할 가능성 확인(POS 시스템은 결제 정보를 처리하고, 네트워크 카메라는 사람의 흐름을 처리하고, 의료 장치는 중요한 데이터를 처리하는 등).



## 2022-2. ORPHE Inc. (하지 근골격계 질환 환자, 의사, 연구자가 신뢰할 수 있는 보행 데이터 유통시스템)

### 【유스케이스 구성도】

- ① W3C VC1 표준에 따라 VC 전문가에게 보행 및 통증 데이터를 제공하여 환자의 데이터 공유가 가능하다. 전문가들은 VC 서명을 통해 환자 데이터를 확인하고 일상 데이터를 온라인으로 공유할 수 있어 효율적인 진료가 가능하다.
- ② Wallet 애플리케이션을 사용하면 의사와 PT가 적절한 범위 내에서 데이터에 액세스할 수 있다.
- ③ Wallet을 사용하면 연구원과 제약 회사가 적절한 환자에게 개인 데이터의 개인정보를 보호하면서 데이터 공유를 요청할 수 있다. 분산 스토리지는 이러한 데이터를 교환할 때 변조 위험을 낮춘다.



### 【검증해야할 데이터】

- 환자들은 (의사, 연구 기관 등) 데이터 공유 요청자가 발행한 관계-가상화폐 서명을 사용하여 요청을 제출한 사용자 속성을 확인한다.
- 누적된 생체 인식 데이터가 해당 환자에 속하는지 확인하기 위해 데이터를 기록하는 동안 신원 또는 센서 데이터를 확인한다 (미래에).
- 환자의 걸음 걸기 측정 및 주관적인 통증 등과 같은 입력 데이터가 조작되지 않았는지 확인하기 위해 분산 저장소 (개인 데이터 레이크 IPFS)에 해시를 기록한다.

적법성 검증	검증 대상	검증 방법	검증자
사용자 속성	접근 사용자의 소속 확인	VC 서명의 검증	환자, 의료전문가, 연구자
데이터가 환자에게 속하는지 여부	보행 측정 및 주관적 통증 등 사용자 입력 데이터	기록시 신원확 인(향후 센서 데이터를 기반으로 한 보행인식)	의료전문가, 연구자
환자 데이터의 조작 방지	보행 측정 및 주관적 통증 등 사용자 입력 데이터	분산 저장소에 해시 기록(개인 데이터 레이크 IPFS)	의료전문가, 연구자

#### 【합의 구축과 추적】

데이터 제공자와 데이터 뷰어는 지정된 기간 동안 데이터를 공유하기로 합의한다. 이를 위해 데이터 제공자는 애플리케이션의 웹 관리 화면에서 발행된 요청을 승인한다. 체결된 합의는 VC 사용 로그를 확인하여 추적할 수 있다. 합의를 취소하거나 데이터를 철회하는 것도 가능하다.

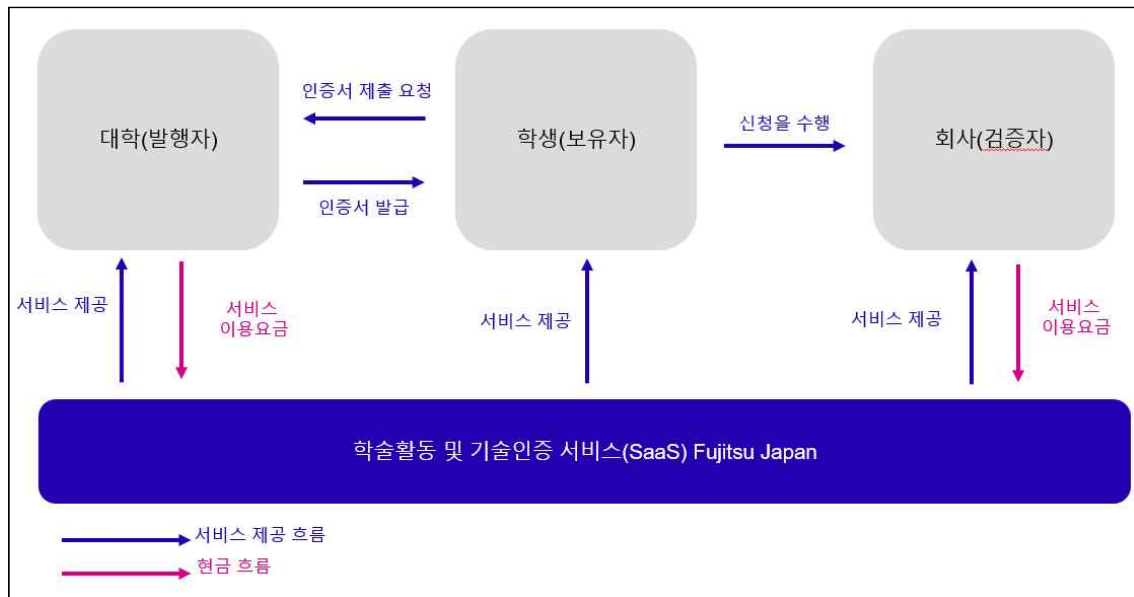
#### 【실험 내용】

- 일부 하지 근골격 질환 환자와의 애플리케이션 구현 및 시범 시연을 통해 시스템의 실현 가능성과 수요를 확인하였다.
- 사용자 속성의 확인 및 환자 데이터의 방해 없음을 검증한 성공적인 구현이다.
- 이 프로젝트는 신발 센서의 데이터에 의존합니다. 레코딩 시점에 환자가 사용자인지 데이터 출처를 확인하기 위해서는 추가적인 연구가 필요하다. 이를 위해 센서 데이터의 보행 인식과 같은 추가 분석 기술의 필요성을 인지하였다.

### 2022-3. 후지쓰 Japan (컨소시엄 “인적자원개발을 위한 신뢰받는 교육정보 유통 시스템”)

#### 【유스케이스 구성도】

- ① 회사는 신뢰할 수 있는 제3자인 상사가 활동을 평가하고 승인함으로써 청구된 학생의 기술 등을 적절하게 확인할 수 있다. 증거가 없는 활동 정보도 신뢰할 수 있는 제 3자에 의해 승인될 수 있다. 이를 통해 효과적인 취업활동이 실현되고 매칭 정확도가 향상된다.
- ② 본 서비스를 이용하면 인증서를 디지털 방식으로 발급받을 수 있으며, 진위 여부를 보장하면서 원스톱 디지털 서비스를 구현하여 인증서 발급기관(대학 등)의 관리비용을 절감할 수 있다.
- ③ 블록체인 기술을 활용하여 변조 위험을 줄이고 문서 교환을 허용한다.



#### 【검증해야할 데이터】

- 감독관은 학생이 요청한 학생의 활동과 기술을 확인하고 그것이 올바른지 승인한다. Fujitsu에서 제공하는 IDYX1과 이에 구축된 애플리케이션에 의해 제어된다.
- 학생이 기업에 제출한 지원서가 허위가 아닌지 확인하기 위해 VC의 서명을 확인하여 지원서의 원본을 확인한다. IDYX에 의해 제어된다.
- 학생과 감독자의 신원확인으 Microsoft의 AD 인증을 사용하여 이루어진다.

필요 검증 발급	검증 대상	검증 발급	검증자
허위활동/기술 신청(학생→지도교수)	학생이 감독관에게 요청한 활동 및 기술에 대한 설명	내용이 맞는지 감독자의 확인 후 확인	관리자
허위활동 및 기술적용(지도교수의 학생평가)	강사가 지원 내용에 추가한 활동 및 능력에 대한 평가 내용	VC가 여러 제3자에 의한 활동 및 기술 인증을 실현한다	채용센터(회사)
신원 검증	학생 및 지도교수의 ID 정보(이름, 소속, 이메일 주소 등)	Microsoft의 Azure AD 인증 기능으로 활성화됨	Azure AD

#### 【합의 구축과 추적】

학생과 지도교수는 기술과 활동을 평가하고 의견을 제시하는 데 동의하였다. 학생이 선언한 기술과 활동이 시스템의 감독관에 의해 승인되면 합의가 형성되는 것으로 간주된다. 이행된 계약은 IDYX 로그를 검토하여 추적할 수 있다.

#### 【실현 내용】

##### 학생의 능력을 포함한 입증이 어려운 학업성취도 증빙서류

- 증명하기 어려운 개별 과목의 구체적인 내용과 능력을 신뢰할 수 있는 사람이 증명함으로써 학생들의 성취가 회사와 정확하게 연결될 수 있다. 그 결과, 개인별로 최적의 취업 지원을 제공하는 것이 가능해진다.
- 지금까지 취업활동에서 증명하기 어려웠던 결과평가(봉사활동, 동아리 활동) 이외의 학업성취도와 능력을 증명하는 것이 가능해졌다.

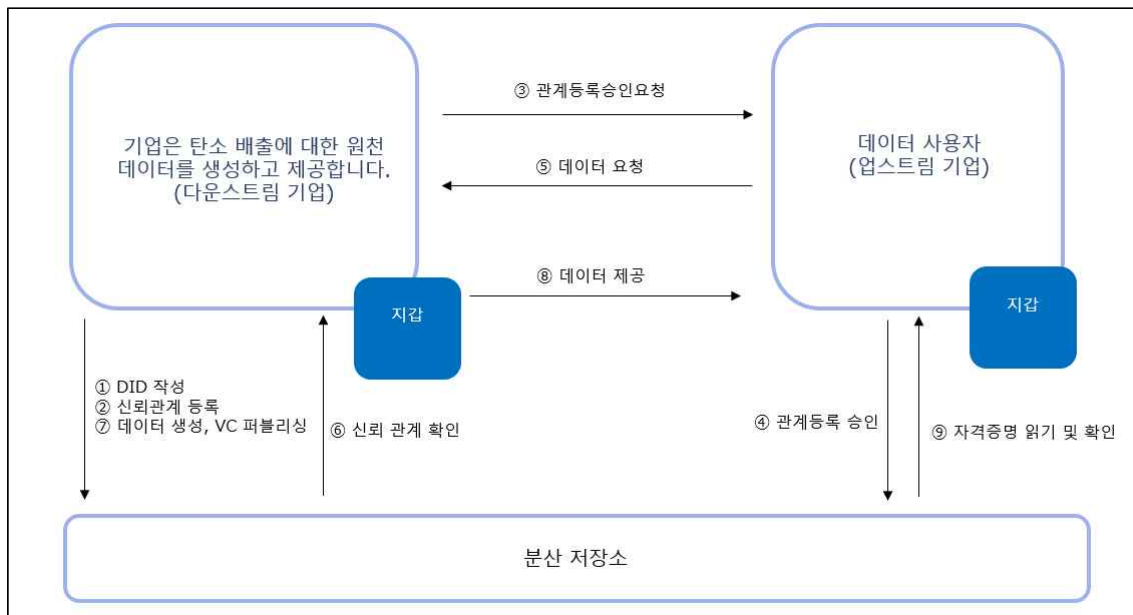
##### 사업 모델 리뷰

- 이미 논문으로 발급되는 성적증명서 등의 증명서보다는 아직 체계화되지 않은 활동이나 기술과 관련된 자격증에 대한 사회적 요구가 더 높은 것으로 나타났다.
- 이 시연에서 채택된 활동 및 기술 등록의 세분성과 관련하여 학생들은 주저 없이 활동 및 기술을 쉽게 등록하고 평가할 수 있으며 회사에 제출할 활동 및 기술을 적절하게 선택할 수 있음이 입증되었다.

## 2022-4. Data Gateway (분산ID를 이용한 탄소배출량 추적시스템)

### 【유스케이스 구성도】

- ① IoT 센서로부터 직접 데이터를 획득하고 처리함으로써, 위조 방지 인증을 받아 안전하게 데이터를 처리할 수 있다. 분산 스토리지를 사용하면 데이터 손실 및 위조 가능성을 줄이면서 통신이 가능하다.
- ② DID 및 보안 계산을 공급망의 다른 사람에게 기밀 데이터를 공개하지 않고도 신뢰할 수 있는 GHG 양을 제공한다. 법인 간 신뢰를 제공하는 자격증명(관계 자격 증명)은 공급망 내 해당 관계를 적절하게 관리하고, 미리 지정된 기간 동안 사전에 파악된 범위 내에서 데이터를 공유할 수 있도록 해준다. 영지식증명은 제공업체의 데이터베이스에서 데이터를 선택한다. 지갑 어플리케이션은 관리자 자신의 결정을 데이터 제공에 직접 반영하고 적절한 내용을 적합한 사람들에게 공유한다.



### 【검증해야할 데이터】

- IoT 센서에서 직접 측정한 데이터를 획득하고 처리하여 분산 스토리지에 저장한다. 이를 통해 데이터 위조가 없는지 검증하고 VC(Verifying Credential)를 통해 데이터가 측정된 위치를 인증할 수 있다.
- 회사 간 공급망 자격 증명은 승인된 회사의 데이터 수집 요청만 허용한다.
- 데이터는 해당 권한 있는 관리자의 승인을 받아 공유된다.

검증 필요 문제	검증 대상	검증 방법	검증자
측정 데이터에 대한 위조 여부 확인	IoT 센서에서 추출된 데이터	VC에서 분산 스토리지 및 해싱으로 분산완료	데이터가 발생하는 회사
다른 회사와의 공급망 관계	기업 간 데이터 연계	관계 자격 증명(VC) 확인	공급망의 각 회사
접속 이용자 식별	접속 이용자 식별	생체 인식	데이터가 발생하는 회사

#### 【합의 구축과 추적】

공급망의 다양한 비즈니스 엔터티는VC를 통해 데이터를 제공하기 위해 그들 간의 관계에 동의한다(관계 자격 증명). VC를 기반으로 데이터 공급자의 관리자는 사용자 회사의 관리자의 신청을 승인하고 합의하게 된다. 체결된 계약은 VC의 사용 로그를 확인하여 추적할 수 있다.

#### 【실현 내용】

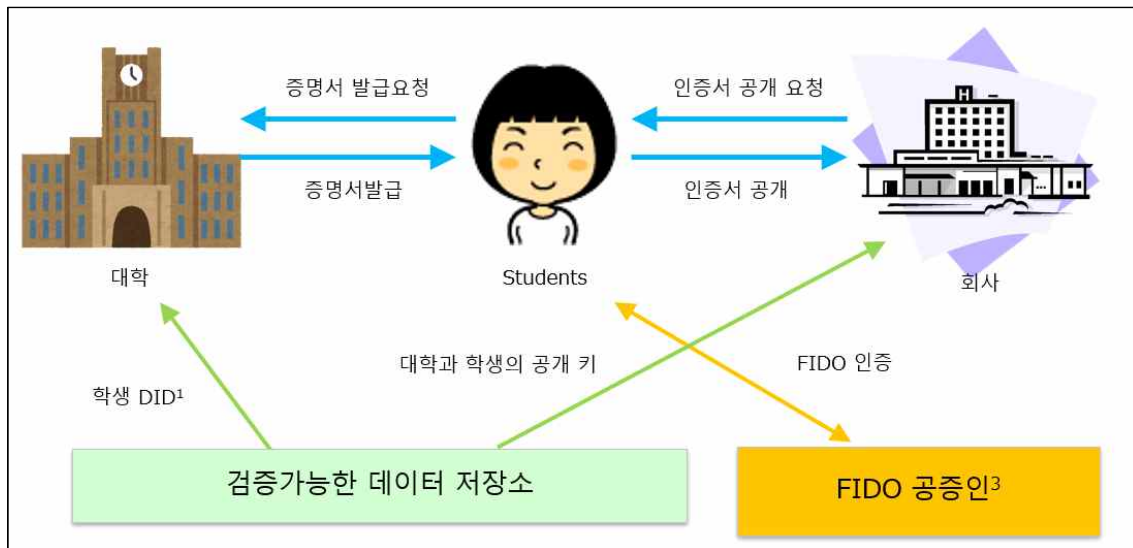
- 시연을 통해 데이터 위조 방지 입증을 위한 손실 허용성 및 보안 측면에서 블록체인의 결합보다 분산형 스토리지와의 결합이 더 유리한 것으로 나타났다.
- 분산 ID와 ZKP(영지식증명)/보안연산을 결합하여 개인정보 및 조직의 기밀정보를 위조 위험 없이 정확하게 기록, 연산, 시각화하면서도 보호한다. 데이터가 암호화된 형태로 사용되기 때문에 여러 조직, 기업에서도 안전하게 데이터 처리가 가능해 기존 온실가스 추적 참여를 꺼렸던 기업도 참여할 수 있다.
- 이제 우리는 이것을 GHG 프로토콜(온실가스 프로토콜: 온실가스(온실가스) 배출량 산정 및 보고에 관한 기준)에서 신뢰할 수 있는 기본 데이터의 구현된 형태로 입증했으므로 업계 협회와 협력하여 이 형식의 국제 표준화를 장려할 수 있었다.

## 2022-5. 도쿄대학 (학력별 개별 관리로 인적자원 흐름 촉진(SSI/FIDO 컨소시엄))

### 【유스케이스 구성도】

학생들은 디지털 학업 증명서를 회사에 제출할 수 있습니다. 대학은 디지털학력증명서를 발급하거나 받을 수 있다.

- 이러한 인증서는 학생(학생 또는 교직원), 대학 및 기업의 관리 비용을 절감한다.
- 대학과 기업은 저렴한 비용으로 디지털학력증명서를 검증할 수 있다.



### 【검증해야할 데이터】

- 대학은 FIDO 공증인에 등록된 ID 토큰 B를 파생하는 ID 토큰 A를 학생에게 발급한다. 학생들은 확인을 위해 B를 대학에 제출하여 신원을 증명한다.
- 학생의 DID는 VDR에 등록되어 기업에 공개된다. 회사는 VDR에서 얻은 학생의 공개 키로 학생의 신원을 확인한다.
- 기업은 VDR에 등록된 대학의 공개 키를 획득하여 학업 증명서를 확인한다.

적법성 검증	검증 대상	검증 방법	검증자
학생 ID	ID 토큰	전자서명	대학
학생 ID	분산형 DID	전자서명	회사
학생 ID	학력증명서(VP)	전자서명	회사

### 【합의 구축과 추적】

학생과 회사는 학업 증명서를 회사에 공개하는 데 동의한다. 학생이 미리 정한 조건

과 기업의 공개 요구가 충족되면 합의된 것으로 간주된다. 체결된 협약(학력공개)은 정보공개일지를 확인하여 추적 가능하다.

**【실현 내용】**

- 자격 증명을 증명하기 위해 키 쌍을 만들고 VDR과 학생 DID에 공개 키를 구현했다. 회사는 학생들의 신원을 확인했다.
- BBS 서명(영지식증명1)을 통해 학생들은 여러 소스에서 필요한 정보를 변조하지 않고 수집하여 자신의 선호도와 정책에 따라 원본 학업 증명서를 작성하고 회사에 제출할 수 있다.



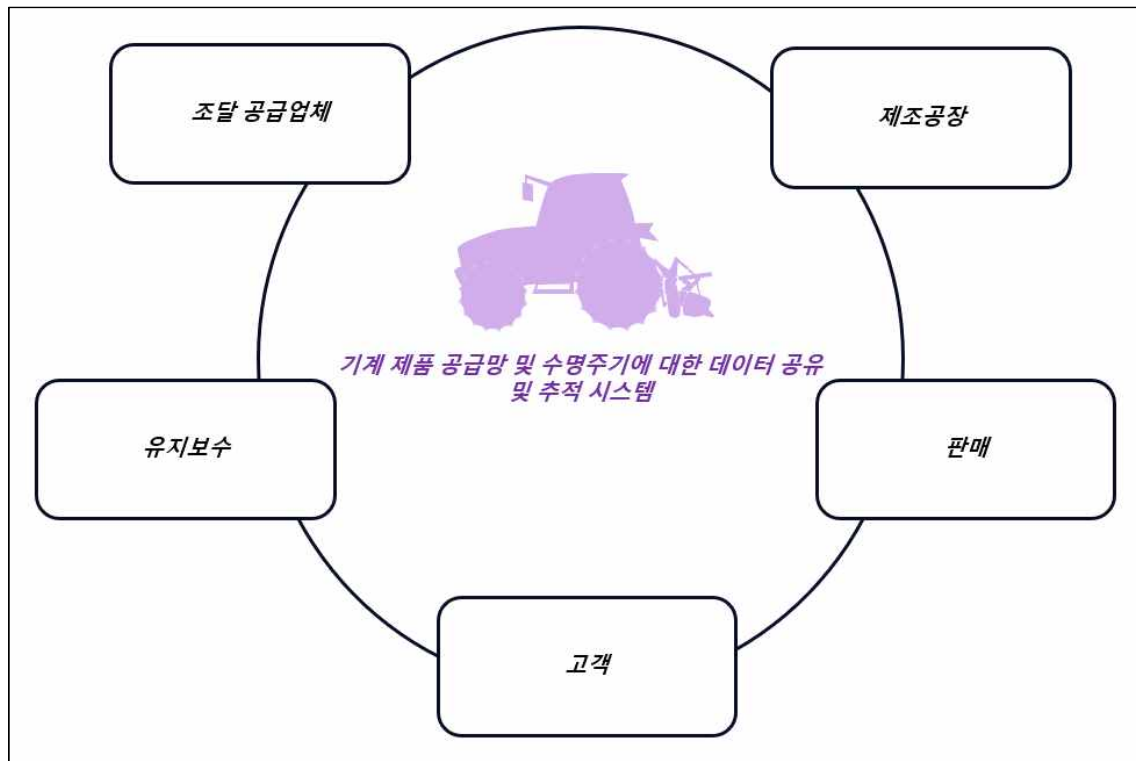
## 2022-6. Yanmar Holings Co.,LTD. (기계 제품 공급망의 추적성 관리)

### 【유스케이스 구성도】

공급망 전반에 걸쳐 해결해야 할 사항

- ① Trusted Web을 사용하면 이해관계자 간에 여러 데이터를 안전하게 공유하고 공급망 전체에서 활용할 수 있다.
- ② 이를 통해 공급망에서 교환되는 데이터의 검증 가능성이 향상되고 이해관계자 간의 신뢰성 높은 교환이 가능해진다.

이 사용 사례에서는 데모를 위해 운영 데이터를 사용한다. 이를 통해 제조업체는 필요한 경우 수리점과 데이터를 안전하게 공유할 수 있다. 특히, 증거검증(기계검증)을 통해 공개 대상의 적법성과 공개 요청에 따른 적절한 데이터 공개가 가능해진다.



### 【검증해야할 데이터】

- 수리점에서 제조업체에 보낸 수리 요청에 포함된 데이터의 적법성을 확인하기 위해 기계 서명을 검증한다. 특히, 기계 서명에 포함된 정보(수리점이름, 기간 등)를 확인하고 요청의 적법성을 확인한다.
- 모든 발신자의 서명을 검증하고 수신자의 확인을 수행하여 교환된 데이터의 적법

성을 확인한다.

적법성 검증	검증 대상	검증 방법	검증자
요청자	기계가 서명했다는 사실	서명확인(기계 서명/제조업체 서명)	제조업체
수리요청	기계 사용자의 요청	서명확인(사용자 서명/정비소 확인)	수리점
제공 데이터	제조업체의 작동 데이터	서명확인(제조업체 서명/정비소 확인)	수리점

#### 【합의 구축과 추적】

- 기계 수리에 관한 기계 사용자와 수리점간의 합의: 계약은 서명 및 조건 교환으로 이루어진다. 컴퓨터 사용자는 사용자 응용 프로그램의 실행 상태를 추적할 수 있다.
- 기계 작동 데이터 열람에 대한 수리점과 제조업체 간의 합의: 제조업체의 기계 서명 확인을 통해 합의가 이루어진다(데이터 제공자(제조업체)가 공개 기간을 관리할 수 있다.).

#### 【실현 내용】

기계 제품 공급망에서 생성된 데이터를 대상으로 기계 수리 현장을 선정하고, 이해관계자 간의 안전한 데이터 교환을 위한 계획 기획 및 프로토타입 제작을 수행했다. 실현 내용은 다음과 같다:

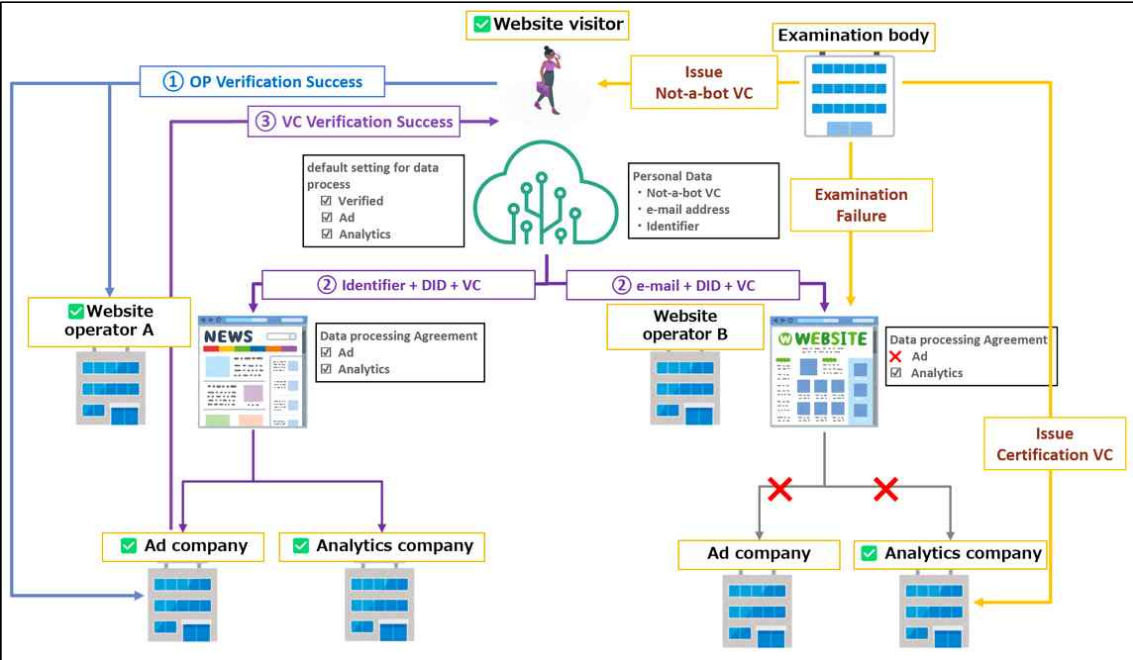
- 기계제품 수리 현장의 계획 기획 및 프로토타입 제작
- 사물(기계)에 ID 제공
- 사물(기계)과 법인/사람의 페어링: 사물과 그 책임 주체를 연결한다.
- 사물(기계)의 추적성 보장: 사물의 DID는 제품 수명 주기 동안 동일하게 유지된다.
- 증거 검증에 따른 데이터 공개 통제: 데이터 공개 대상 및 근거 확인
- 신원 가시 범위의 제한 : 사용자 정보의 가시성 제한

2022-7. DataSign Inc. (온라인 마케팅에서의 개인 데이터 분포)

【유스케이스 구성도】

소비자가 자신의 개인 데이터를 제어할 수 있는 메커니즘을 구축하고, 해당 데이터를 사용하는 업체의 정당성과 데이터 신뢰성을 검증할 수 있도록 한다.

- ① 소비자는 온라인 마케팅에서 사용되는 자신의 식별자와 그 목적지를 관리한다.
- ② 각 당사자는 정당한 제3자로부터 발급된 인증을 통해 상호 검증한다.
- ③ 정당성과 검증 검사 실패 시, 당사자 간에 사례별로 합의가 이루어진다.



【검증해야할 데이터】

개인 데이터의 부적절한 획득 문제를 해결하기 위해, 당사의 정당성이 검증된 경우 데이터를 신속하게 전달해야 함. 광고 사기 대책에 관해서는, 웹사이트 운영자와 광고 기술 운영자는 웹사이트 방문자에게 비봇인증을 제공해 접근을 확인 함.

정당성 검증 필요	검증 대상	검증 방법	검증자
웹사이트 방문자 데이터의 부적절한 획득	웹사이트 운영자와 광고 기술 운영자	인증기관이 발행한 웹사이트 운영자용 OP를 검증	웹사이트 방문자
봇에 의한 광고 사기	웹사이트 방문자	비봇인증기관이 발행한 비봇VC를 검증	웹사이트 운영자와 광고 기술 운영자

#### 【합의 구축과 추적】

개인 데이터 사용 범위에 관해서는, 사전 합의된 조건을 기반으로 기능을 개발하여 검증된 당사자에게만 데이터를 신속하게 제공. 해당 당사자의 획득과 사용은 추적되며, 필요한 경우 합의 철회로 비활성화 됨.

#### 【실현 내용】

- DID3/VC/DWN4/OP의 사용을 통해 현재 온라인 마케팅에서 개인 데이터 배포 문제를 해결할 수 있는 실제 시스템을 구축하여 증명
- Originator Profile (OP)를 사용하는 조직을 검증하고, 범용 기능에 대해 연구. OP의 부족한 부분에 대한 피드백을 제공함으로써 OP의 향후 사용 사례에 기여.
- DID, VC 및 DWN 라이브러리 대부분이 개발 중이기 때문에 기능과 규칙이 충분하지 않은 수준에서 개발이 어려움. 표준 규격에 기반하여 구체적인 코드를 구현한 후, 오픈 소스 코드의 현재 부족한 부분과 도전 과제를 발견. 이를 바탕으로 완성된 코드를 제공하고 오픈 소스 개발 커뮤니티에 기여.

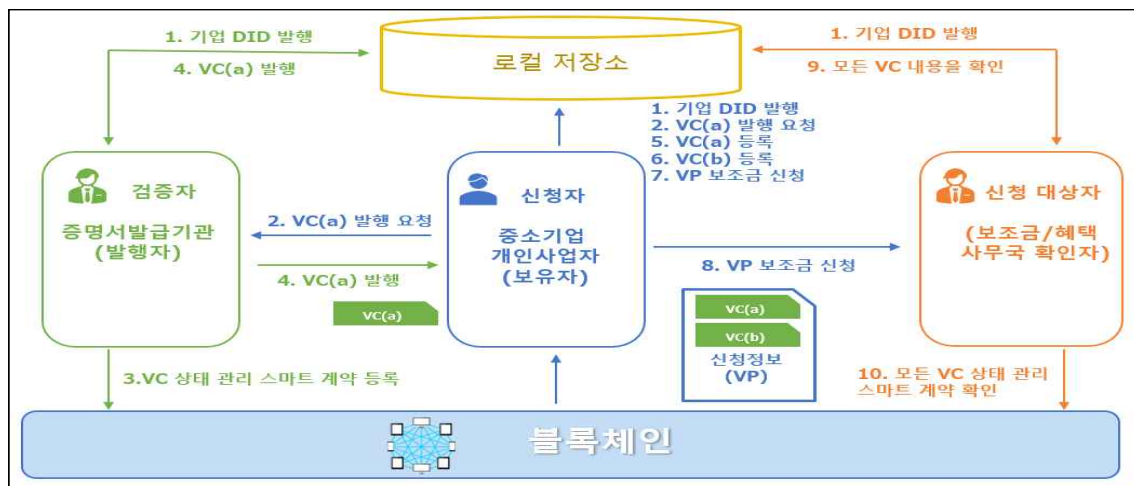
## 2022-8. DENTSU (중소기업 및 개인사업자의 온라인 보조금 신청을 위한 “신원 및 존재 증명”을 위한 새로운 시스템)

### 【유스케이스 구성도】

웹 애플리케이션을 통한 디지털화 방식, VC에 의한 검증 가능한 디지털 인증서 발급, 블록체인 기반 인증 상태 관리 등을 통해 비용 절감을 실현하고 애플리케이션 정보의 신뢰성을 향상시킨다.

- ① VC는 인증서의 디지털 발급을 가능하게 하며 진위성을 보장하고 인증서 내용 검증에 드는 비용을 절감한다. 웹 애플리케이션은 각 당사자의 주관적인 정보 공개 및 다양한 애플리케이션을 가능하게 한다. 웹 응용 프로그램에서 인증서를 사람이 관리하고 제출함으로써 불완전한 응용 프로그램 문서를 수정하기 위해 교환하는 횟수가 줄어 든다.
- ② 다른 보조금 신청의 기존 데이터를 재사용하여 여러 신청 상태 관리를 간소화한다.
- ③ 블록체인을 활용하면 VC 발행 이후 인증자의 재량에 따라 해당 VC를 무효화(사기, 자격취소 등)하는 것이 가능하다.

위의 장점을 공공과 민간 모두에 활용하고 도입함으로써 사회의 디지털 정보 신뢰성 향상과 향후 전반적인 행정 비용 절감을 기대할 수 있다.



### 【검증해야할 데이터】

#### 지원자 사칭 및 지원서 내용 위조

지원자 사칭 여부를 확인하기 위해 VC 서명 검증을 통해 지원 서류 발급자를 확인한

다. 구체적으로, Benefits Execution Office가 받은 모든 VC는 EdDSA서명으로 확인된다. 또한 VC를 제외한 각 엔터티간의 상호 작용은 JWS 서명으로 확인된다. 서명 검증은 통해 발급기관이 어디인지, 내용의 변조 여부 등을 확인할 수 있어 검증 영역이 확대된다

- ① 검증할 적법성: 데이터에 서명하여 변조되지 않도록 데이터 전송을 검증함
- ② 검증 대상(데이터/데이터 거래): 엔터티와VC 간의 상호 작용은 서명을 통해 검증됨
- ③ 검증 방법: EdDSA및 JWS의 검증을 받음
- ④ 검증자: (신청) 수신자 및 모든 데이터 수신자
- ⑤ 데이터 소유권: 인증자및 신청자(VC), 신청자 및 신청 수신자(VP)
- ⑥ 발행자: 지방자치단체, 금융기관, 세무서(인증자)
- ⑦ 데이터(VC) 저장 : 현재 로컬 저장소에 저장되어 있음
- ⑧ 액세스 제어 방법: 앞으로는 보낸 사람과 받는 사람만 메시지에 액세스할 수 있음
- ⑨ 결과/주의 사항 : 서명검증을 통해 영역을 확장할 수 있음

#### 【합의 구축과 추적】

신청자가 제공한 정보와 보유정보가 일치하는 결과를 바탕으로 합의가 이루어진다. 위 동의에 대해 신청자와 검증자는 로컬 저장소의 데이터를 읽어 승인된 각 메시지의 상태를 추적할 수 있다. VC 상태는 블록체인의 스마트 계약으로 관리되므로 VC 상태가 취소될 수 있다.

#### 【실현 내용】

- Trusted Web을 활용한 메커니즘을 통해 기존 보조금 및 혜택 신청 프로세스를 디지털화하기 위한 기술 연구에서 기존에 종이 인증서 또는 스캔 데이터를 첨부하여 수행되었던 식별 및 존재 증명을 EdDSA서명을 확인하여 구현하였다. 주민등록증 VC, 계좌유지증명서 VC, 납세증명서 VC이다. 그 결과, VC의 발행권한과 내용이 위조되지 않았음을 성공적으로 확인하였고, 구현이 기술적으로 가능함을 확인하였다. 원격 식별, 프라이빗서비스를 포함한 기존 KYC 방식과의 연계 등 보다 효율적인 방식을 고려할 필요성이 확인되었다.
- 비즈니스 모델 연구를 위해 이해관계자 인터뷰 결과를 바탕으로 다음과 같이 제안한다.
  - ① 디지털 인증의 장점과 단점(비용 절감 및 시스템 운영 부담 증가)
  - ② 인증자의 서비스 수수료 수입 등의 이점
  - ③ 생태계 조성 노력의 중요성 및 아날로그(종이) 기반 세계에서 전환하는 데 드는 비용

## 2022-9. 일본정보기술서비스산업협회(JISA) (법인세 제도 및 산업 협회 증명서)

### 【유스케이스 구성도】

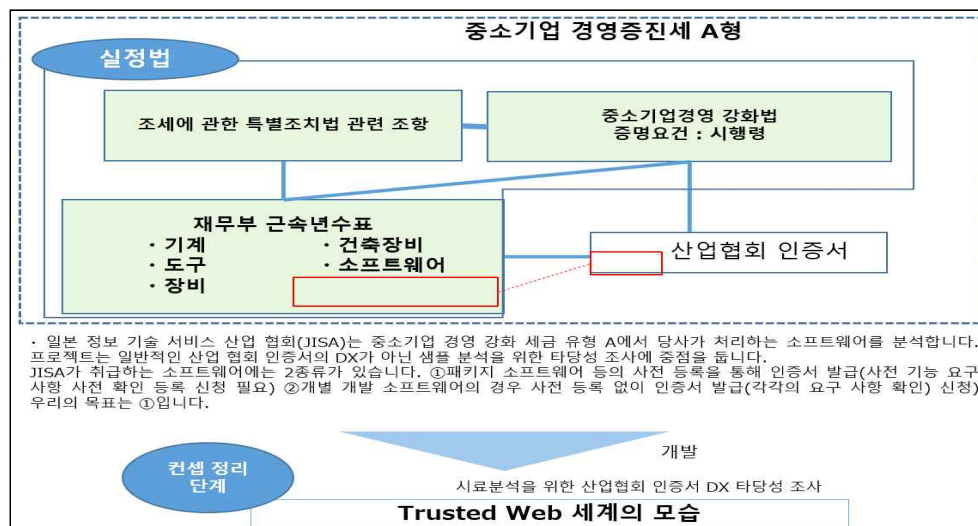
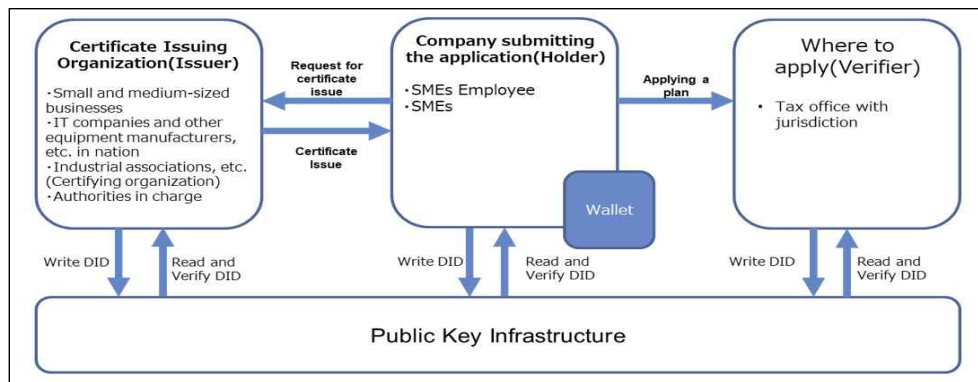
VC를 디지털 인증서로 활용하여 업무 효율성을 위한 절차를 디지털화하고 문서 제출의 신뢰도를 높인.

#### ① 신청서 및 서류의 디지털화

- 중소기업은 브라우저 기반 웹애플리케이션을 통해 디지털화된 시스템에서 산업 협회 인증서를 신청할 수 있다.
- 중소기업은 웹애플리케이션을 이용해 디지털인증서(VC)와 문의내용을 연동하고 확인할 수 있다.

#### ② VC를 통해 애플리케이션 데이터 등의 신뢰성을 확보할 수 있다.

- JISA는 SME의 신청이 요구 사항을 충족하는지 확인한 후 SME에 디지털 인증서(VC)를 발급할 수 있다.
- 중소기업은 세무서 등이 요청한 귀속자료를 VC가 신속하게 제출할 수 있다.
- VC(Tamper-Free)가 제공한 인증은 세무서 등에서 확인할 수 있다.



## 【검증해야할 데이터】

Verification subject	Verification method	Verifier	Data owner	Issuer	data place	Access control	Results / Points to be noted
①Identity about the enterprise (and natural persons related to the enterprise) [enterprise VC]	Verify the four types of certificates on the left and the certificate issuer	①SMEs, etc.	SMEs, etc.	①SMEs, etc.	① Application Server ② Wallet	The actors with access to storage in this use case are SMEs and their employees.  Access control to storage is done by Enterprise VC.	<ul style="list-style-type: none"> <li>· Add proof of affiliation information (date of enrollment confirmation, confirmation method) to the Enterprise VC so that it can verify that the applicant really belongs to the company.</li> <li>· G-Biz ID is not currently available to private companies, so bind DNS and DID</li> <li>· Transaction IDs and authorization numbers enable tracing of VC transactions and VC relationships</li> </ul>
②Description of software used by the company [Use of SW VC]		②IT companies and other equipment manufacturers, etc. in nation ⑤Tax office		②IT companies and other equipment manufacturers, etc. in nation			
③certificate issued by an industrial association [Industrial association certificateVC]		③Industrial associations such as JISA ⑤Tax office		③Industrial associations such as JISA			
④Certification of Accreditation from the Small and Medium Enterprise Agency [Plan accreditation VC]		④Small and Medium Enterprise Agency ⑤Tax office		④Small and Medium Enterprise Agency			

## 【합의 구축과 추적】

합의 주체	<ul style="list-style-type: none"> <li>• 중소기업 및 중소기업 직원</li> <li>• 국내 중소기업, IT기업, 기타 장비 제조사 등</li> <li>• 중소기업 및 JISA 등 산업협회(인증기관)</li> <li>• 중소기업 및 담당관청(중소기업에 대한 관할권)</li> <li>• 중소기업 및 담당세무서</li> </ul>
합의 목적	본 Usecase에는 시나리오 적용에 필요한 서류 및 정보에 대해 "제출"과 "수락"의 과정이 있으며, 각각 "제출"과 "수락"의 과정이 완료되면 합의로 간주된다.
계약 조건	합의된 속성과 자격 증명이 전달됨
추적 목적	위의 계약이 이행되었음을 확인
추적 주체	기업 및 임직원
추적 방법	VC 발행 및 제시 내역을 회사 및 임직원이 사용하는 Wallet에 보관하여 열람할 수 있도록 한다.
계약의 철회 여부 및 방법	<p><b>VC가 취소된 경우</b></p> <p>발행자는 발행된 VC를 취소할 수 있다. VC를 취소한 후에는 발급자와 검증자의 검증으로 인해 보유자는 새로운 인증서 발급을 신청하거나 VC에 새로운 인증서를 제시할 수 없다.</p> <ul style="list-style-type: none"> <li>• VC가 이미 인증서를 신청하거나 제시한 경우, 철회가 발생했다고 인정한 검증자의 재검증을 거쳐 계약이 철회된다. (이미 신청했거나 제시한 다수의 VC에 대한 일괄처리에 대해서는 지속적인 고려가 필요할 것으로 추정된다.)</li> </ul> <p><b>계약이 취소된 경우</b></p> <ul style="list-style-type: none"> <li>• VC 발행 또는 제시에 대한 동의를 확인할 때 보유자 측이 계약을 취소하는 경우 VC의 취득 또는 제시 프로세스는 수행되지 않는다.</li> <li>• 발행자 또는 검증자 측이 계약을 취소하는 경우(예: 제시된 VC의 만료), 보유자에게 VC 획득/제시 프로세스가 실패했음을 통보한다.</li> </ul>

## 【실현 내용】

이번 시연을 통해 디지털 적용에 있어 향상된 편의성과 JISA 산업인증 적용에 있어서 VC의 신뢰성 확보 타당성을 검증할 수 있다.



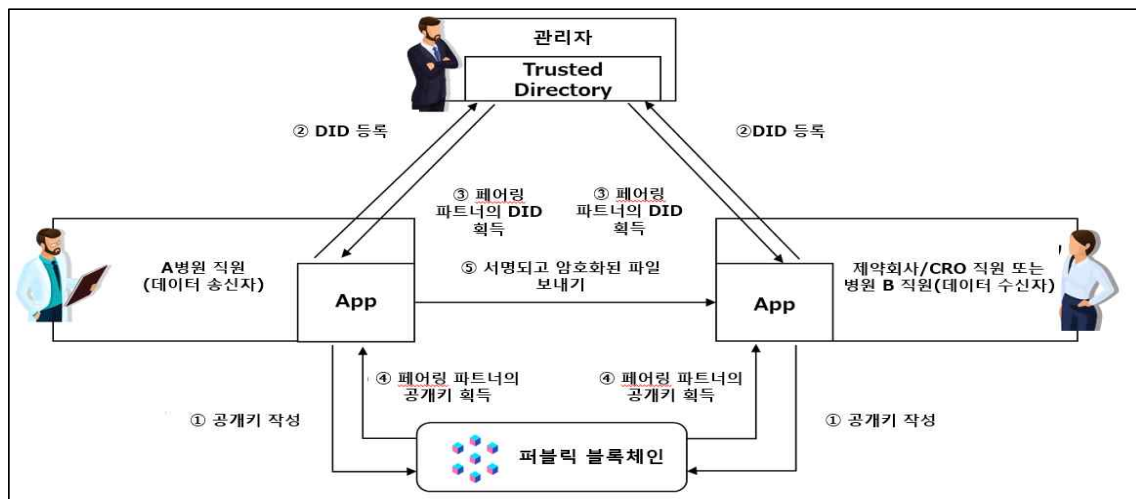
2022-10. 시믹 (임상시험 및 의료현장에서 신뢰성과 적용성이 높은 정보 유통 시스템, 의료정보 유통시스템 개발 컨소시엄)

【유스케이스 구성도】

Keychain Core의 블록체인 프레임워크와 당사자의 디바이스와 연계된 DID를 구현하여 페어링을 수행한 당사자 간에 암호화된 파일을 독점적으로 전송하는 시스템을 구축한다. 이를 통해 정보의 신뢰도를 높이고 편의성을 향상시켰다.

- ① 디지털화된 시스템을 통해 종이 매체의 관리 및 운영 비용을 절감한다.
- ② 여러 파일(데이터)을 신뢰할 수 있는 사용자에게만 보이는 형태로 암호화하고 교환하는 다목적 시스템을 구축하여 구현이 용이하다.
- ③ 당사자의 기기에 연결된 DID를 구현하여 사칭 위험을 줄이고, 페어링을 수행한 당사자 간에 암호화된 파일을 독점적으로 교환하는 시스템으로 안전성을 보장하고 변조를 방지한다.

이 시스템의 설계는 DID를 사용하여 사용자가 정보를 능동적으로 제어하고 신뢰할 수 있는 사용자를 동적으로 관리할 수 있도록 한다. 이는 병원 간, 환자와 병원 간 적절한 정보 교환을 실현하는 플랫폼이 될 수 있다.



【검증해야할 데이터】

- 송신자는 송신 데이터(임상 테스트 데이터 포함)에 서명하고 암호화하여 데이터가 변조되지 않도록 보호한다.
- 수신된 암호화된 데이터는 페어링을 수행한 송신측의 DID가 데이터를 암호화했는지 확인하여 확인할 수 있다.

적법성 검증	검증 대상	검증 방법	검증자
전송된 데이터(임상 시험 데이터가 포함된 파일의 내용)를 변조하지 않음	서명 및 암호화된 파일	서명 검증 및 복호화 가능	제약회사/CRO 직원
명의 도용 금지	서명 및 암호화된 파일	페어링된 DID와 동일한 DID로 서명 및 암호화 됨	제약회사/CRO 직원

#### 【합의 구축과 추적】

데이터 송신자(병원 직원)와 수신자(제약사/CRO 직원)는 “서로 신뢰 가능”, “데이터 전송”에 동의한다. 데이터 송신자와 수신자가 복호화 가능한 DID 목록 파일(신뢰할 수 있는 당사자 목록)을 확인한 후 서명 및 암호화를 검증하고 서명 검증을 수행함으로써 합의가 이루어진다고 가정한다. 암호화 이력(감사추적)을 확인하여 체결된 계약을 추적할 수 있다.

#### 【실행 내용】

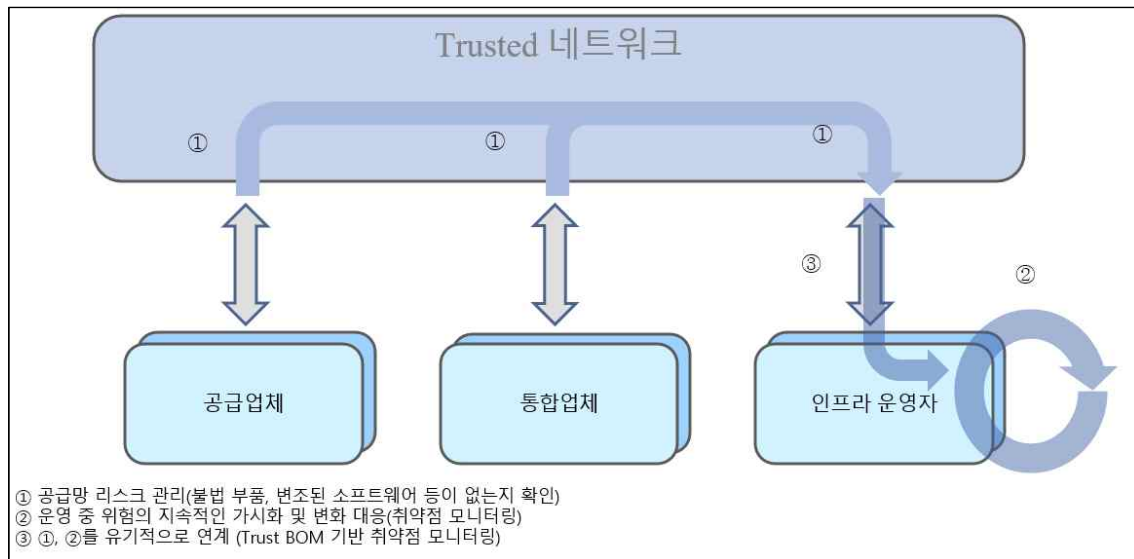
실증 기간 동안 실제 의료기관 네트워크와 Souseikai글로벌임상연구센터(Souseikai)와의 네트워크 간 프로토타입 시스템의 현장 테스트를 진행하였다. 또한, 내·외부 전문가 및 이해관계자 인터뷰를 진행하였다. 이번 현장 테스트와 인터뷰를 통해 얻은 결과, 제안, 의견은 다음과 같다.

- (결과) 현장 테스트는 문제 없이 완료되었으며 예상되는 거동 및 효과가 확인되었다. (의견/의미) Souseikai의 반응은 저비용 계획 및 구현이 필요하고 현재 데이터 무결성을 보장하지 않는 의료 기관 및 학계에서 수행하는 임상 연구 및 역학 연구에 시스템을 도입하고 싶다는 것이었다. 구현에 많은 비용이 소요되는 시험 및 연구에 대해 기존 프로세스 자체를 크게 변경하지 않고 프로세스 내 작업 내용을 단순화함으로써 저비용 모델 구현 가능성이 제시되었다.
- (의견) 우리는 프로토타입 시스템의 아키텍처와 이를 통해 얻을 수 있는 이점이 미래의 모습을 보여주는 예가 될 것이라고 생각한다. 반면, 현재 의료 현장과 임상시험에서 요구되는 데이터 무결성 개념에 비해 지나치게 엔지니어링됐다는 느낌도 든다. 따라서 우리는 이 프로토타입 시스템의 아키텍처와 Trusted Web 백서에서 요구하는 기술 요구 사항을 사회 전체에 전파하는 활동이 필요하다고 생각한다.

## 2022-11. ALAXALA Networks Corporation (Trusted Network를 통한 소셜 IT 인프라의 신뢰도 및 탄력성 향상 실현)

### 【유스케이스 구성도】

- 조달하는 IT기기의 Trust BOM 정보를 변조나 유출 없이 유통할 수 있는 안전한 플랫폼(Trusted Network)을 구현하고, 실제 제품과 비교하여 변조나 취약점을 점검할 수 있다.
- 신뢰성 데이터는 DID·VC를 사용하여 정보를 보거나 변경할 권한이 있는 사람만 접근해야 한다.
- 위의 제품 신뢰성 정보를 벤더, 통합업체, 인프라 운영업체 전반에 걸쳐 원스톱 방식으로 제공하는 플랫폼(신뢰할 수 있는 네트워크)을 구현한다.



### 【검증해야할 데이터】

DID/VC를 활용하여 제공된 상품이 변조되지 않았는지(정품성) 검증한다.

- 제품 구성 정보(예: HBOM/SBOM, 장치 일련번호, 소프트웨어 해시 값)
- 애플리케이션 소유자의 디지털 인증서(NFT)
- 실제 제품에 RFID 부착

위의 정보를 비교하여 진위 여부를 확인한다. 제품의 Trust BOM 정보의 진위 여부는 VC의 서명을 통해 확인할 수 있다. 이러한 정보에 대한 기록 내역은 블록체인에 기록되며, 변조가 불가능하다.

적법성 검증	검증 대상	검증 방법	검증자
제품 정품성	제품정보 DID/VC, 실제 제품의 일련번호	제품정보(HBOM/SBOM 등의 구성정보, 일련번호 등), 제품 소유자 정보(NFT)를 실제 제품에 부착된 RFID 값과 일치시킨다. 제품 정보의 진위 여부는 VC를 통해 확인할 수 있다.	인프라 운영자, 통합자

#### 【합의 구축과 추적】

상품에 대한 거래 계약이 체결되어 계약이 체결되었다고 가정한다. TBOM(HBOM/SBOM) 합의 구축과 연계하여 데이터 소유권/접근 권한 이전 VC 사용 로그를 확인하여 추적 가능한 계약을 이행한다.

#### 【실현 내용】

##### Trusted Web 유스케이스 생성 및 시연

- Trusted Web의 활용 사례로 IT 장비 조달 공급망에서 IT 제품의 정품 여부를 확인하는 메커니즘(Trusted Network)을 계획하고 검증하였다.

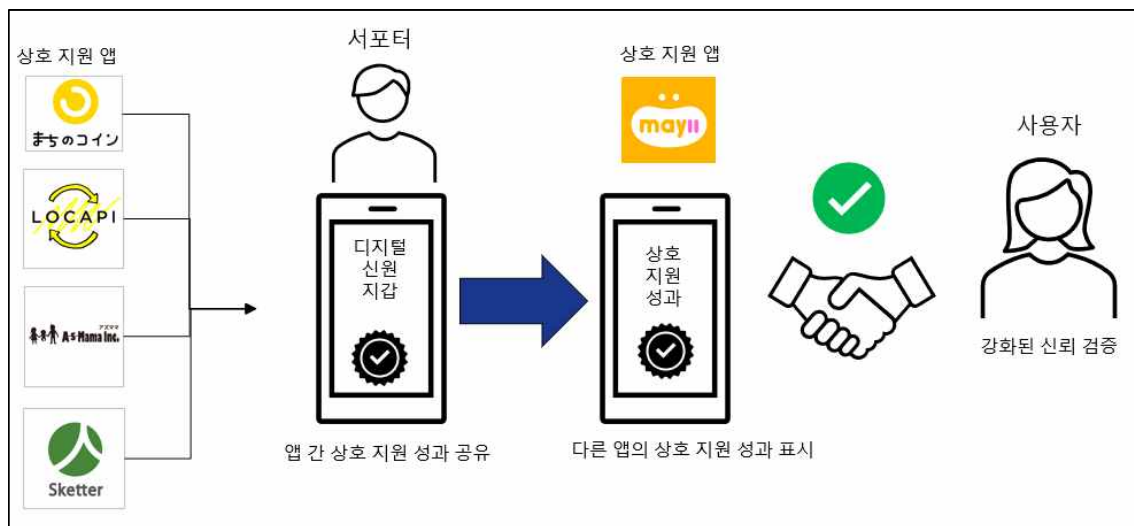
##### Trusted Web 유스케이스 프로토타입

- Trusted Network의 프로토타입이 개발되었으며, Trusted Web의 요구 사항을 충족하는 시스템으로 OKINAWA Open Laboratory에서 프로토타입에 의한 가치 증명을 통해 기대한 대로 작동함을 검증하였다.

## 2022-12. 대일본인쇄(DNP) (사용자 신뢰 공유 상호 지원 애플리케이션)

### 【유스케이스 구성도】

- ① 이용자는 자신의 개인정보를 보호하면서 자신의 데이터를 관리하고 제3자에게 제공할 수 있다. 이를 통해 데이터 입력량을 늘리지 않고도 신뢰 검증 범위를 이전보다 강화할 수 있다.
- ② 도움을 원하는 사용자는 디지털 인증서로 발급된 상호 지원 활동 결과를 바탕으로 자신의 필요에 맞는 서포터를 선택할 수 있다. 데이터는 단순히 자체 보고된 정보보다 훨씬 신뢰할 수 있다.
- ③ 300개 이상의 서비스 공유 어플리케이션 간에 정보를 공유함으로써, 다른 앱에서 상호지원 앱으로 제공되는 축적된 성취 데이터를 신뢰 검증에 사용할 수 있다. 지원 회원에 대한 인센티브 강화로 대학입시, 취업활동 등에서 성취도를 검증할 수 있는 시스템을 구축한다.



### 【검증해야할 데이터】

- 상호지원 앱 내 활동 실적을 디지털 증명서로 발급한다. 후원자의 신뢰를 높이기 위해 VC 서명으로 성과의 진위 여부를 확인한다. 특히, 공조 앱 A에서 발행한 VC는 다른 공조 앱 B에서 검증하게 된다.

적법성 검증	검증 대상	검증 방법	검증자
프로필 필드에 허위 선언	공조 VC의 정확성	VC 서명 검증	기타 공조앱(제3자)
공조활동 허위 선언	공조 활동 성과 VC	VC 서명 검증	대학, 기업(제3자)

미래의 새로운 가치를 창출하기 위해, 대학이나 기업에 공조 활동 성과를 위한 디지털 증명서 제출을 상정하고 있다.

#### 【합의 구축과 추적】

- 사용자는 다른 앱에 저장된 데이터의 가용성과 범위를 선택하여 다른 상호 지원 앱과 공유하고 합의할 수 있다.
- 공조 어플리케이션 Wallet에서 공유된 공조 달성 VC 이력에 대해 사용자는 해당 데이터를 공유한 내용과 당사자를 추적할 수 있다.
- 지자체의 활성 데이터 영역(상호지원 앱 사용 기록 기반)을 추출 및 분석하고 지역 과제를 해결한다.

#### 【실현 내용】

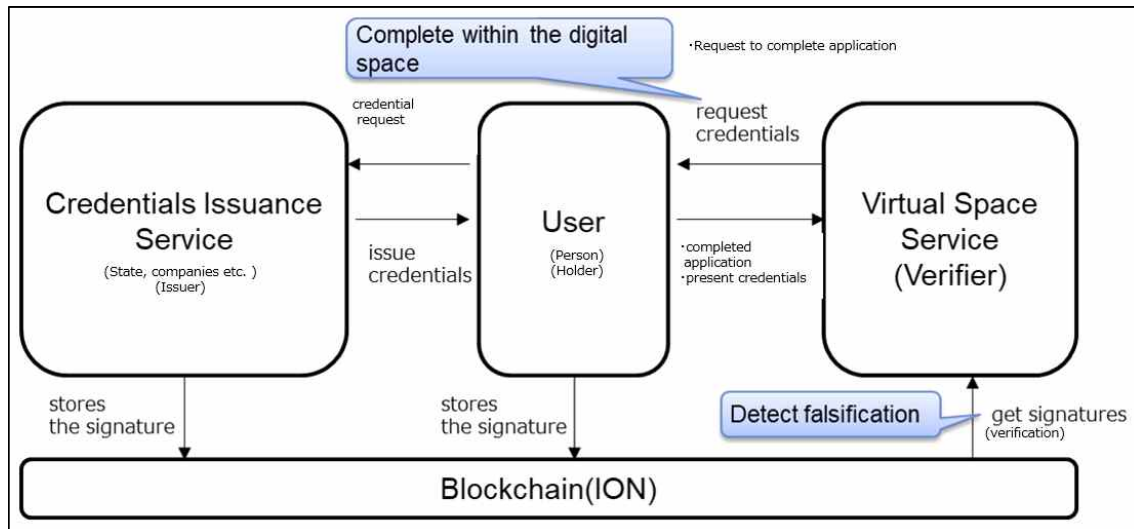
- 시스템 기획 및 개발 시연을 통해 "보안 문제의 명확화"와 "사용자의 개인 키 복구 방법"이 필요하다는 것을 깨달았다. 보안 문제를 명확히 하면서 VC와 DID 모두에 대한 우려를 연구했다. 독일의 ID 이상 연구 결과를 바탕으로 '스스로 회복', '집중 회복', '신뢰할 수 있는 제3자에 의한 회복', '복구 불가능(복구 불가)'의 4가지 방향을 정리하였다. Cloud Wallet을 활용하여 '집중복구' 방식을 채택할 예정이다.
- 비즈니스 모델 시연에서는 '안전성', '인식', '계속 사용(인센티브)', '수익화'에 대한 4가지 이슈가 있다. 상호지원 앱의 에코시스템을 구축함으로써 “안전성”과 “지속적인 사용(인센티브)”에 기여할 수 있다.
- 상호 도움 신뢰 프레임워크의 공식화에 대한 시연을 통해 “A. 상호지원 신뢰체계의 항목을 명확히 한다”, “나. 상호협력 신뢰 프레임워크 형성의 의미”, “다. 각 이해관계자의 역할을 명확히 한다”, “라. 상호 도움 신뢰 프레임 워크의 공식화에 관한 문제”. 실제 사용자가 사용하는 앱의 신뢰 인증 기준 및 UI/UX에 대해서는 여전히 이슈가 있어 D항에 대한 연구를 계속할 예정이다.

## 2022-13. NRI Digital (가상현실 공간에서의 서비스 적격성 및 제공 데이터 신뢰 검증)

### 【유스케이스 구성도】

DID/VC 및 지갑 애플리케이션을 사용하면 다음과 같은 자격 증명 제출 및 확인을 완료할 수 있다.

- ① 사용자는 가상공간 서비스에서 DID/VC와 Wallet의 자격증명 발급 서비스를 통해 발급받은 자격증명을 제출할 수 있다.
- ② 서비스 제공자는 가상 공간에서 자격 증명을 수신하고 블록체인에 작성된 서명을 확인하여 자격 증명(위조 감지)을 확인할 수 있다.



### 【검증해야할 데이터】

- 가상 공간에서 제공되는 서비스는 범죄수익 양도 방지법 등 법률에 따른 이용 자격 여부를 확인하기 위해 본인 확인이 필요하다.
- 신원확인을 올바르게 수행하려면 자격 증명의 진위가 필요하다. 구체적으로는 발급자(Credential Issuer)로부터 받은 정보를 VC로 만들어 사용자가 이를 가상 공간에서 서비스 제공자에게 제출하고, 서비스 제공자는 가상 공간에서 VC의 진위 여부를 검증한다.

적법성 검증	검증 대상	검증 방법	검증자
허위 자격증명을 이용한 서비스 이용, 사칭	사용자 자격 증명의 진위성	VC 서명 확인	가상공간 서비스 제공자

#### 【합의 구축과 추적】

- 이용자(가상공간상의 이용자)와 발급자(신뢰정보발급기관), 이용자와 검증자(가상공간 서비스 제공자)는 수신되는 각 데이터 내용의 내용에 대해 합의한다.
- 사용자와 발급자간, 사용자와 검증자간 각각의 계약을 체결한다. 이러한 상태는 수신된 데이터의 동의 내용을 Wallet에 표시하고 확인함으로써 추적된다.

#### 【실현 내용】

메타버스 특유의 개인정보 보호 문제를 연구하였다. 우리는 Metaverse에서 사용자 자격 증명 확인과 개인 정보 보호를 모두 충족하는 수단이 필요하다는 것을 배웠다. 우리는 Trusted Web이라는 아이디어를 확산시키기 위해 수익화 문제를 연구했다. 결과는 다음 2개 항목이다.

- Trust 정보를 발행하는 서비스 제공자인 Issuer에 대한 수익화 모델이 필요하다.
- 발행자가 임시 정보 사용 수수료를 검증자에게 전달하더라도 발행된 Trust 정보에 대한 데이터 추적성을 보장하는 시스템이 없으면 발행자는 특정 비용으로 해당 정보에 대한 Trust 발행에 대한 수익을 창출하지 않는다.



## 2. 2023년 「Trusted Web 실현을 위한 유스 케이스 실증 사업」 공모 채택 결과

	유스 케이스 이름	사업자명	분야
1	지갑을 통한 신원 관리 및 온라인 커뮤니케이션	DataSign	개인
2	공동 앱에서 플랫폼을 넘어 사용자 트러스트 공유	대일본 인쇄	개인
3	국제간의 교육 확충과 노동 시장의 유동성을 높이는 신뢰 네트워크 구축	Institution for a Global Society	개인(인재)
4	대학 기술 직원의 활약을 향한 스킬의 보이기화: 스킬의 질 보증과 주체적 정보 공개의 시험	후지쯔 Japan	개인(인재)
5	해외 인재 환류에 있어서의 크로스보더형 개인정보 유통 시스템	PitPa	개인(인재)
6	제조 공급 체인에서 제품 함유 화학 물질 정보 등의 확실한 전달을 가능하게하는 Chemical Management Platform (CMP)	미즈호 리서치 & 테크놀로지스	공급망
7	사업장 ID와 그 디지털 인증 기반	SBI 홀딩스	공급망
8	임상시험 및 의료현장에서의 신뢰성 및 응용 가능성이 높은 정보유통시스템(해당분야 : 의료·헬스케어)	시믹	건강 관리
9	하지 운동기 질환 환자와 의사, 연구자 간의 신용할 수 있는 보행 데이터 인증·유통 시스템	ORPHE	건강 관리
10	KYC / KYB 기반 트러스트가있는 거래를 촉진하는 새로운 메커니즘	덴츠 국제 정보 서비스	법인, 금융
11	보조금 사업을 소재로 한 법인용 행정 절차 DX 사회 기반화의 사전 검토	정보서비스산업 협회	행정
12	Trusted Web Advertising System with OP	Originator Profile 기술 연구 조합	미디어

※ 출처: TOPPAN SOCIAL INNOVATION website, “「令和4年度補正 Trusted Web の実現に向けたユースケース実証事業」に関するお知らせ”, [https://www.toppa.n.com/ja/joho/social/trusted\\_web2https://solidproject.org/023\\_koubo.html](https://www.toppa.n.com/ja/joho/social/trusted_web2https://solidproject.org/023_koubo.html)

## <첨부 2> 일본: Trusted Web Framework 분석

### 1. Trust Architecture, Trust Framework, SSI의 정의

트러스트 아키텍처는 기업, 기관 또는 생태계 내에서 다양한 주체 간의 상호 작용과 정보 교환을 지원하기 위한 구조와 프로토콜의 집합이다. 시스템이나 소프트웨어 아키텍처 내에서 신뢰를 구축하고 유지하기 위한 설계와 구조로, 주로 기술적인 측면을 강조하며, 보안, 인증, 권한 부여, 암호화 등과 같은 기술적 요소를 활용하여 시스템 내의 신뢰성을 보장한다. 보안 레이어 및 구성 요소를 정의하고, 이들 간의 상호작용과 데이터 흐름을 설계함으로써 신뢰성을 확보할 수 있다.

트러스트 프레임워크는 디지털 환경에서 신뢰성을 확립하고 유지하기 위한 지침과 표준의 모음이다. 더 넓은 범위의 개념으로, 기술적인 측면 뿐만 아니라 조직 문화, 정책, 규정, 이해관계자 간의 협력 등을 포함한다. 조직 간, 시스템 간, 개인 간 등 다양한 관계에서 신뢰를 구축하기 위한 원칙, 가이드라인, 규정을 제공한다. 기술적 측면 뿐만 아니라 비즈니스 프로세스, 법적 규제 준수, 개인정보 보호 등을 다루며, 시스템 및 기술의 외부 요소도 고려해야 한다.

자기주권 신원증명(SSD)은 개인이 자신의 디지털 신원을 소유하고 관리할 수 있는 체계를 의미한다. 탈중앙화된 기술과 암호화를 활용하여 개인이 자신의 신원 정보를 안전하게 보호하고 필요한 경우에만 제 3자와 공유할 수 있게 해준다. 트러스트 프레임워크는 신뢰할 수 있는 지침과 규정을 제공하고, SSI는 이를 구현하는 기술적 체계로 볼 수 있다.

### 2. Trust Framework

“Trusted Web”은 규정과 합의 형성, 추적 등을 위한 요건을 충족시키기 위해 기술적 프로토콜로는 해결되지 않는 문제가 있다. 이러한 문제를 보완하기 위한 거버넌스가 중요하다. 따라서 Trusted Web에 적합한 거버넌스 구조를 탐구해야 한다. 디지털 비즈니스의 네트워크 효과, 증가 수익 및 감소 비용 등의 요인은 쉽게 독점과 과도한 기업 활동에 의존하며 락인효과가 발생할 가능성이 크다. 락인효과는 경제학에서 사용되는 개념으로 시장에서 특정 기업이나 제품이 경쟁자들에 비해 더 높은 점유율을 보이거나 시장에서 지배적인 위치를 확립할 때 발생하는 현상으로 이로 인해 경쟁사들이 새로운 진입이나 경쟁을 어려워하게 되어 시장의 경쟁이 저해되거나 억제되는 상황을 의미한다. 디지털 인프라에서 새로운 신뢰 프레임워크를 구축할 때, 공동 자산에 적합한 거버넌스 구조를 고려하는 것은 오늘날의 문제점이 재발하는 것을 방지하기 위해 필수적이기 때문에 전 세계적이고 기술 중립적인 인터넷 거버넌스가 동일하

게 적용되어야 한다. 표준화, 구현, 운영, 커뮤니티 형성 등의 활동에 다양한 이해 관계자들을 참여시키는 것 또한 중요하다.

## 2.1. 거버넌스의 중요성

Trusted Web은 기술적인 기반(인프라)으로서 기능을 전 세계적이고 기술 중립적으로 제공하는 것이 목적이다. 다른 한편으로, Trusted Web에서 제공되는 응용프로그램은 각 국가의 기존 법률 체계와 비즈니스 관행으로 구성된 신뢰 메커니즘과 필요에 따라 조화를 이루어야 한다.

## 2.2. 거버넌스의 핵심 개념

- **다중 이해 관계자 지향**: 분산 방식으로 지원되는 다양한 경로 및 그 체인은 다양한 이해 관계자들이 협력하여 전체 시스템으로 구성된 신뢰를 지탱한다. 다양한 이해 관계자들의 합의 구축을 통해 전체 시스템이 정상적으로 작동될 수 있는 지속 가능한 거버넌스가 마련되어야 한다.
- **정부의 역할 재정의**: 신뢰 앵커의 역할을 수행하며, 디지털 사회 활동을 지원하기 위한 규칙을 개발해야 한다.
- **투명성, 추적성, 감사성**: 합의 구축의 과정, 결과 및 결과물을 기록하여 다양한 이해 관계자들이 확인하고 검증할 수 있도록 하여 악의적인 참가자들이 전체 시스템의 신뢰를 무너뜨리는 것을 방지해야 한다.
- **생태계를 지속 가능하게 하는 인센티브 디자인**: 공동 자산을 구축하고 운영하는 역할을 하는 사람들을 위한 인센티브를 고려해야 한다.

## 3. Trusted Web에서 실현하고자 하는 것

비즈니스 시 데이터 컨트롤 능력을 사용자에게 제공하고 데이터 검증 능력을 확보하는 것이 Trusted Web 시스템에 필수적인 기능 중 하나이다. Trusted Web은 안정성 향상 및 신뢰성 보장 등을 추구하며, 가능성과 문제를 다룬다. 이러한 내용에는 경제적 효과를 평가하기 어려운 것들이 많이 있다. 하지만 검증된 인증서(VC)를 재사용하면 신청/승인 프로세스가 간소화되어 경제적인 이점이 있을 수 있다.

[표 24] Trusted Web의 실현 목표 및 효과

데이터 주체	Trusted Web의 실현 목표	실현 효과
개인, 법인	• 데이터 컨트롤 능력 확보	데이터 홀더의 안정성 향상

개인, 법인	• 데이터 증명자(증명 데이터 발급자) 검증성 확보	데이터 증명자의 신뢰성 담보, 데이터 홀더의 안정성 향상
개인, 법인	• 검증자(데이터 제시 대상) 검증성 확보	데이터 증명자의 신뢰성 담보, 데이터 홀더의 안정성 향상
개인, 법인	• 데이터 홀더의 검증성 확보	데이터의 신뢰성 확보, 데이터의 활용 촉진
개인, 법인, 사물	• 데이터 검증성 확보	데이터의 신뢰성 확보, 데이터의 활용 촉진
개인, 법인	• 데이터 공유 및 제시와 관련된 합의 형성	정확한 데이터 거래 실현
개인, 법인	• 검증 정보, 검증 결과 재사용	신청, 검증 작업에 관련된 공수 및 비용 절감
개인, 법인, 사물	• 데이터 수집 강화	데이터의 신뢰성 확보, 데이터의 활용 촉진
사물	• IoT 디바이스의 ID 프로비저닝 효율성	기기 관리자 비용 절감, 취약성 제거
사물	• 디바이스의 신뢰루트 구축•디바이스의 암호키관리	암호화 키 관리 설계 개발 비용 절감

#### 4. Trusted Web 구현 기능 및 구조

많은 기업들이 분산 스토리지 및 지갑을 사용하여 데이터 분산 관리를 채택하고 있다. 또한 대부분의 기업들이 DID 발급 기능을 구현하고 있으며, 데이터 분산 관리와 결합하여 데이터 자체 제어를 실현하는 유스케이스가 많이 있다.

[표 25] Trusted Web 구현 기능 및 실현 수단

기능, 비기능	구현 기능	실현 수단
기능	데이터 분산관리 (데이터 등록 및 취득)	DWN, IPFS 등의 분산 스토리지 관리, 지갑 애플리케이션으로 관리
	분산 식별자(DID) 발급	지갑 및 각 회사 미들웨어 기능(CG EDGE, IDYX, Woollet, Keychain 등)으로 구현
	검증 가능한 속성 정보, 인증서 발행, 관리, 검증	VC, OP 구현

	데이터의 선택적 공개	BBS+서명 등
	본인 확인 · 실재 증명	Microsoft Azure AD, 생체인증 등
	암호화 키, 검증 생성 및 관리	지갑 및 각 회사 미들웨어 기능(CG EDGE, IDYX, Woollet, Keychain 등)으로 구현
	메시지 트랜잭션 기록	블록체인에 DID(Document) 등록, 지갑 저장소에 메시지 트랜잭션 데이터 저장
	메시지 및 트랜잭션 추적	메시지 및 트랜잭션 기록 검증 및 확인
	데이터 교환에 대한 합의 형성	시스템·애플리케이션의 UI(승인 의뢰·승인)로 구현
	데이터 교환에 대한 합의 취소	스마트 계약
비기능	가용성	오프라인에서도 자신의 속성 정보나 공개 이력에 액세스 가능한 구성, 시스템 가동률 확보 등
	확장성	엔티티 수에 따른 확장성 확보
	보안	데이터의 기밀성 확보 등

## 5. Trusted Web 데이터 제어 거버넌스

대부분의 기업(11/13)은 데이터를 분산 관리 또는 일부분산 관리 형태로 채택하고 있다. 반 이상의 기업에서 데이터 홀더에 의한 선택적 공개를 구현하고 있으며, 또한 구상 외/검토 중인 기업에 대해서는 최근의 요구가 없기 때문에 구현에 대한 기술적 장벽은 크지 않을 것이다.

다음은 13곳의 대표기관별 데이터 관리 형태를 확인하고, 선택적 공개를 구현하고 있는지 데이터 거버넌스는 어떻게 되는지 살펴본다.

### 5.1. DataSign

- o 데이터 관리 형태(분산 · 집중): 분산적으로 개인이 관리, 발급된 비봇증명 VC나 자신의 개인 데이터를 DWN 및 브라우저 익스텐션에 저장하고 관리한다.
- o 선택적 공개 구현: 사이트 이용자는 식별자와 연결된 속성을 관리하고, 개인 데이터 및 개시 대상, 이용 목적의 범위를 선택하여 공개한다.
- o 데이터 거버넌스: 조직 심사 기관(JICDAQ 등)이 사이트 운영자, 광고 기술 사업자의 정당성에 대해 심사한다. OP가 검증된 정당한 웹사이트 운영자에게만 액세스 권한을 부여한다.

### 5.2. NRI 디지털

- o 데이터 관리 형태(분산 · 집중): 일부 분산적으로 개인이 관리한다. 암호 키 등 일부 데이터에 대해서는 사용자 동의 하에 백업 서비스 제공자가 관리한다.
- o 선택적 공개 구현: 계획 없음.
- o 데이터 거버넌스: 정보 없음. 가상 공간 서비스 제공자의 거버넌스가 존재한다고 가정한다.

### 5.3. 동경대학교

- o 데이터 관리 형태(분산 · 집중): 분산적으로 개인이 관리. 학습자가 자신의 학습 데이터를 PLR 앱으로 관리한다.
- o 선택적 공개 구현: PLR 앱을 확장하여 여러 DID를 관리 가능하게 하여, 학습자가 DID나 VC를 포함하는 데이터의 범위 등을 선택하여 게시한다.
- o 데이터 거버넌스: 정보 없음

### 5.4. 후지쓰 일본

- o 데이터 관리 형태(분산 · 집중): 분산적으로 개인이 관리. IDYX 내의 지갑에서 관리한다.
- o 선택적 공개 구현: 데이터의 선택적 공개는 일부 가능하며, 특정 스킬 및 활동 내의 정보 비공개 제어는 불가능하도록 프로토타입을 구현한다.
- o 데이터 거버넌스: 정보 없음

### 5.5. 시믹

- o 데이터 관리 형태(분산 · 집중): 부분 분산 관리. 데이터 송수신이 가능한 병원 직원 및 제약회사/CRO 직원의 조합 정보는 Trusted Directory에서 집중적으로 관리한다.
- o 선택적 공개 구현: 보내는 파일에 어떤 데이터를 넣을지는 병원 직원이 직접 선택 가능하며, 어떤 파일을 보낼지도 선택 가능하다.
- o 데이터 거버넌스: GAMP (Good Automated Manufacturing Practice) 등 임상 시험에서의 데이터 관리 및 시스템 설계에 관한 국제 표준 및 규제에 의한 전체적인 거버넌스의 영향이 시사된다.

## 5.6. ORPHE

- 데이터 관리 형태(분산 · 집중): 일부는 개인적으로 관리. 환자가 자신의 보행 데이터를 지갑에서 관리하면서, ORPHE가 관리자 시스템에서 데이터 로그를 기록한다.
- 선택적 공개 구현: 환자는 (ORPHE를 통해) 의사 등으로부터 데이터 요청을 받아, 데이터의 공개, 거절, 일부 공개를 지갑에서 선택할 수 있다.
- 데이터 거버넌스: 시스템 전체의 데이터 수신은 ORPHE가 담당하며, 일정한 거버넌스가 존재한다고 가정한다.

## 5.7. DataGateway

- 데이터 관리 형태(분산 · 집중): 기업에서 분산 관리. 클라이언트의 에이전트 서버(지갑: Woollet)에서 클라이언트에 의해 IPFS에 저장된 데이터의 해시를 관리한다.
- 선택적 공개 구현: 선택적 공개는 지갑(Woollet)의 기능으로 구비한다.
- 데이터 거버넌스: 데이터 소유자와 데이터 요청자간의 탄소 배출량 공개에 관한 계약에 따른 거버넌스 기반으로 예상된다.

## 5.8. 안마

- 데이터 관리 형태(분산 · 집중): 분산 관리, 각 엔티티의 데이터는 해당 엔티티에서 보관하며, 필요한 경우 직접 공개 요청을 받는다.
- 선택적 공개 구현: 앱(지갑) UI에서 공개 대상과 기간을 선택할 수 있다.
- 데이터 거버넌스: 기계 사용자의 본인 확인은 기계 제품 구매 시 판매 업체에서 실시한다고 가정한다. 이때 기계 제품과의 페어링도 실시된다.

## 5.9. Alaxala Networks

- 데이터 관리 형태(분산 · 집중): 분산 관리, 체인 공급망에서 각 엔티티가 안전한 스토리지(IPFS)에서 분산적으로 관리한다.
- 선택적 공개 구현: 장비를 조달한 사업자에게만 선택적으로 개방한다. 권한 관리 메커니즘은 독자적으로 구현한다.

- o 데이터 거버넌스: 데이터 처리 등은 TNP 운영자와 이용자 간의 계약에 따라 규정될 것으로 예상된다.

#### 5.10. 도시바테크

- o 데이터 관리 형태(분산 · 집중): 집중 관리. 문서 관리 시스템 내에서 관리됨. MFP 장치가 식별자 (DID)를 발급하고 전자 문서 등의 속성 (데이터)으로 관리한다.
- o 선택적 공개 구현: 계획 없음.
- o 데이터 거버넌스: 데이터 처리는 MFP 기기 도입 기업 (관리자)과 서비스 제공자 (도시바테크) 간의 계약서 등으로 합의한다.

#### 5.11. JISA

- o 데이터 관리 형태(분산 · 집중): 분산 관리. 법인 및 직원의 월렛으로 VC를 관리한다.
- o 선택적 공개 구현: 계획 없음.
- o 데이터 거버넌스: 정부 프로젝트와의 협력 필요성을 제기하고 있으며, 미래에는 정부에 의한 거버넌스도 고려하고 있다.

#### 5.12. 텐쓰

- o 데이터 관리 형태(분산 · 집중): 집중 관리. 신청자가 수집한 증명서 등 (VC)은 공통 로컬 스토리지에서 관리한다.
- o 선택적 공개 구현: 신청자 자체적인 선택적 공개는 향후 검토 예정이다.
- o 데이터 거버넌스: 언급 없음. 공통 로컬 스토리지의 관리자에 의한 거버넌스가 예상된다.

#### 5.13. 대일본인쇄

- o 데이터 관리 형태(분산 · 집중): 분산적으로 법인으로 관리. 클라이언트의 에이전트 서버 (지갑 : Woollet)에서 클라이언트가 관리한다.
- o 선택적 공개 구현: 자격증명으로 필요한 정보만 선택적으로 공개하는 것을 가정한다.



- 데이터 거버넌스: 공조판의 트러스트 프레임워크에 따른 거버넌스의 필요성을 제기하였다.

## 6. Trusted Web 합의 형성 및 추적

### 6.1. DataSign

- 합의 주체: 웹 사이트 이용자와 사이트 운영자 및 광고 기술 사업자 간
- 합의 대상: 웹 사이트 이용자의 개인 데이터 (광고 식별자, 이메일 주소)의 이용 범위
- 합의 취소: 가능. 정보 제공 철회로 DWN 상의 VC를 삭제할 수 있다.
- 추적 대상: DWN에 저장된 웹 사이트 이용자의 개인 데이터 수집 기록. 기록 조회만으로 실제 이용 여부는 추적 불가능하다.
- 추적 방법: DWN 접근 기록 확인

### 6.2. NRI 디지털

- 합의 주체: ① 지갑 (메타버스 사용자) 및 발행인, ② 지갑 및 가상 공간 서비스 (사업자)
- 합의 대상: ① VC로 발행하는 본인 자격 정보의 내용, ② 요구하는 본인 자격 정보의 내용 및 이용 용도
- 합의 취소: 계획 없음. ① UC는 필요 없다고 판단하였고, ② 폐기 요청해도 정말로 폐기했는지 확인할 수 없기 때문이다.
- 추적 대상: 합의한 사실
- 추적 방법: ①②에서 이행된 합의를 지갑에서 확인하고, VC 발급/제시 이력으로 지갑 내에 표시한다.

### 6.3. 동경대학교

- 합의 주체: 학습자와 기업 간
- 합의 대상: 속성 정보 공개 가능
- 합의 취소: 가능
- 추적 대상: 데이터 교환. 데이터 공개 요청, 그에 대한 동의/비동의 등의 이력

- 추적 방법: 공개 요청 및 공개의 이력 공유

#### 6.4. 후지쓰 일본

- 합의 주체: 학생 및 지도 교사 및 교수
- 합의 대상: 스킬 및 활동에 대한 평가 및 코멘트
- 합의 취소: 계획 없지만 기술적으로는 가능하다.
- 추적 대상: 합의한 사실. 목적지(기업 측)에서 정확히 수령되고 검증되었는지를 학생 자신이 추적한다.
- 추적 방법: IDYX로 증거를 유지

#### 6.5. 시믹

- 합의 주체: 데이터 송신측(병원 스태프)과 수신측(제약 회사 / CRO 스태프)
- 합의 대상: 서로 신뢰하고 있으며 신뢰하는 사이에서 데이터 교환
- 합의 취소: 가능. 클라우드 스토리지(BOX)에 있는 암호화된 파일을 관리자가 삭제함으로써 합의를 취소할 수 있다.
- 추적 대상: 합의한 사실
- 추적 방법: 감사 증거 확인

#### 6.6. ORPHE

- 합의 주체: 환자와 의료기관(의사) · 연구기관
- 합의 대상: 환자의 보행 데이터 공유
- 합의 취소: 가능. 월렛으로 실현한다.
- 추적 대상: 합의한 사실
- 추적 방법: 월렛의 기능으로 실현한다.

#### 6.7. DataGateway

- 합의 주체: 공급망의 파트너 기업간
- 합의 대상: 기업간의 관계, 탄소 배출량의 공유
- 합의 취소: 가능. 파트너 기업간 합의한 관계 크레덴셜을 취소함으로써 실현한다.

- 추적 대상: 공유된 데이터의 흐름
- 추적 방법: Woollet의 기능으로 실현한다.

#### 6.8. 얀마

- 합의 주체: ① 기계 사용자 및 수리 상점, ② 수리 상점 및 제조업체
- 합의 대상: ① 수리 내역 (수리 위치, 비용, 납기), ② 가동 데이터 공개
- 합의 취소: 가능. 합의 철회는 철회 합의로 실현된다.
- 추적 대상: 합의한 사실
- 추적 방법: ① 기계 사용자가 앱에서 확인 (트레이스), ② 제조업체가 제조업체 앱에서 확인 (트레이스)

#### 6.9. Alaxala Networks

- 합의 주체: 벤더, 인터그레이터, 인프라 사업자, Trusted Network(TN) 운영 담당자 간
- 합의 대상: 등록 제품 및 서비스 목록, 평가 보고서, 제품 신뢰 정보(TBOM), 제품 신뢰 정보의 레이팅 내용
- 합의 취소: 가능. 계약에 따른 시스템 내 취소 처리를 수행할 수 있다.
- 추적 대상: 합의된 사실, TBOM의 내용 및 소유권 이전 상태
- 추적 방법: 블록체인에 합의된 데이터를 기록하고, 권한을 가진 사용자(DID로 식별)가 이력을 확인할 수 있다.

#### 6.10. 도시바테크

동의 형성 및 이행의 추적은 유스케이스의 특성 상 적용되지 않는다(적용이 어려움). 데이터 거래 이력(특정 MFP 장치에서 언제 어떤 사용자가 전자화 문서를 보관했는지)에 대해서는 문서 관리 시스템의 로그를 확인하여 추적 가능하다.

#### 6.11. JISA

- 합의 주체: 중소기업 및 설비 제조업체, 공협회, 중소기업청, 관할 세무청간
- 합의 대상: VC 제시 및 제시 대상. 신청자에 의한 VC 제시 대상 확인을 바탕으로 합의한다.

- o 합의 취소: 계획 없음
- o 추적 대상: 합의한 VC가 제시 대상에 전달되었음을 확인한다.
- o 추적 방법: 법인 및 직원이 이용하는 Wallet 내 VC 발행 및 제시에 관한 기록을 실시한다.

#### 6.12. 텐쓰

- o 합의 주체: 신청자와 증명자간
- o 합의 대상: VC 신청 내용
- o 합의 취소: 가능. 스마트 계약을 이용하여 후에 VC의 취소가 가능하다.
- o 추적 대상: 교환된 모든 메시지. VC의 유효 상태 확인에 활용한다.
- o 추적 방법: 로컬 스토리지 상의 데이터 읽기

#### 6.13. 대일본인쇄

- o 합의 주체: 협조 어플리케이션 사용자 간, 협조 어플리케이션 간
- o 합의 대상: 정보 제공 가능 여부, 제공 가능한 정보, 정보 제공 가능한 제3자, 제공한 정보의 유효 기간, 협조 어플리케이션 간의 실적 평가
- o 합의 취소: 계획 없음
- o 추적 대상: 협조와 관련된 정보 (VC)의 유통량. 지역의 과제나 상황의 모니터링에 활용을 예상하고 있다.
- o 추적 방법: 언급 없음

### 7. Trusted Web 구현 상세, 속성 정보, 본인 확인, 실재 증명

데이터 속성 인증 방법으로는 대부분의 기업(11/13)이 VC의 서명 검증을 채택하고 있다. 본인 확인 및 실재성 증명에 대해서는, Azure AD의 인증 기능이나 스마트폰의 생체 인증 기능을 채택하고 있는 기업도 있지만, 채택을 고민하고 있는 기업도 많다.

#### 7.1. DataSign

- o 속성 정보 기법: 속성 정보의 인증 방법으로는 DID/VC(비-bot 인증) 및 OP(사이트 운영자, 광고 기술 사업자)를 사용한다.
- o 본인 확인, 실재 증명 방법: 사이트 이용자의 본인 확인에 대해서는 언급되어 있

지 않다. 사이트 운영자, 광고 기술 사업자의 실재성은 JIQDAQ 등의 심사 기관에 의한 심사 결과에 따라 실재성을 증명하는 것을 가정한다.

## 7.2. NRI 디지털

- 속성 정보 기법: 속성 정보의 증명 방법으로는 DID/VC를 사용. 미리 합의하고 ID 연계가 필요한 OIDC보다 VC의 제시에 의한 자격 증명을 수행하는 것이 효과적이다.
- 본인 확인, 실재 증명 방법: VR 고글을이용한 “이용자의 본인 인증“을 “몰입감을 유지한 채“ 실현하는 것을 과제로 삼아 해결 방법을 검토하고 있다. 미리 PIN 코드를 결정하고 인증 타이밍에 VR 공간에 인증 기능을 표시하고 제스처로 화살표 방향을 입력하는 방법으로 해결 가능하다고 가정한다.

## 7.3. 동경대학교

- 속성 정보 기법: 속성 정보의 증명 방법으로 DID/VC를 사용한다.
- 본인 확인, 실재 증명 방법: 학생의 본인 확인을 위해서는 대학 등에서의 실제 인증을 활용한다. 대학 등에서의 실제 인증에 기반하여 FIDO 인증을 통해 특정 기기와 연결된 DID를 기업·대학 등에 제시함으로써 본인 인증을 강화한다.

## 7.4. 후지쓰 일본

- 속성 정보 기법: 속성 정보 증명 방법으로 DID/VC를 사용한다. 후지쓰의 분산형 ID 솔루션인 IDYX의 서비스 내에서 제공된다.
- 본인 확인, 실재 증명 방법: 학생, 지도 교사, 채용 담당자의 본인 확인 방법으로 Microsoft의 Azure AD 인증 기능을 이용한다.

## 7.5. 시믹

- 속성 정보 기법: DID 및 서명 검증을 통해 안전한 데이터 공유를 구현한다. 속성 증명은 실시하지 않으므로 VC는 구현하지 않는다.
- 본인 확인, 실재 증명 방법: 시스템 이용의 전제 조건으로, 임상시험 등을 실시하는데 필요한 각종 규제 요구 사항에 따라 본인 확인 및 실존성 확인이 요구된다.

사용 시 일회용 비밀번호를 사용하여 본인 인증을 검토할 수 있다.

#### 7.6. ORPHE

- 속성 정보 기법: DID/VC는 속성 정보 증명 방법으로 사용된다.
- 본인 확인, 실재 증명 방법: 사용자 접근에 대한 본인 확인으로 스마트폰 생체 인증 기능을 사용한다.

#### 7.7. DataGateway

- 속성 정보 기법: 속성 정보의 증명 방법으로 DID/VC를 사용한다.
- 본인 확인, 실재 증명 방법: 향후 G Biz ID를 사용하여 기업의 실재 확인을 등록하는 방법을 구현하는 것을 고려한다. 사용자 확인을 스마트 폰이나 PC의 생체 인식으로 수행하는 방법을 고려한다.

#### 7.8. 안마

- 속성 정보 기법: 속성 정보의 인증 방법으로 DID와 서명 검증을 사용한다. VC의 사용은 명시되어 있지 않다.
- 본인 확인, 실재 증명 방법: 기계 사용자의 본인 인증은 기계 구매 시 판매 대리점에서 실시하며, 그때 기계 제품과 페어링을 진행한다.

#### 7.9. Alaxala Networks

- 속성 정보 기법: 속성 정보의 증명 방법으로 DID/VC를 사용한다.
- 본인 확인, 실재 증명 방법: TN 이용 계약 체결 및 이용자 등록 시 본인 확인 및 실재 증명을 실시한다.

#### 7.10. 도시바테크

- 속성 정보 기법: 속성 정보의 증명 방법으로 DID/VC를 사용한다.
- 본인 확인, 실재 증명 방법: 정보 없음

### 7.11. JISA

- 속성 정보 기법: 속성 정보의 인증 방법으로 DID/VC를 사용한다. VC 발행 기반으로 Microsoft Azure를 사용한다.
- 본인 확인, 실재 증명 방법: 어떤 기업의 소속 직원의 존재 확인 방법으로 자기 확인이 이루어졌다는 것을 알 수 있지만, 자세한 방법에 대해서는 언급하지 않았다. 기업의 실존성에 대해서는 G Biz ID의 활용을 미래적으로 검토할 예정이다.

### 7.12. 텐쓰

- 속성 정보 기법: 속성 정보의 증명 방법으로 DID/VC를 사용한다.
- 본인 확인, 실재 증명 방법: 신청자의 본인 확인은 시군구에서 대면으로 주민등록증 발급을 통해 실시한다. 이전에는 종이 증명서 또는 스캔 데이터를 첨부하여 본인 확인이나 실존 증명을 진행했으나, 주민등록증 VC, 계좌 실존 증명 VC, 납세 증명서 VC의 EdDSA 서명을 검증하는 방법을 고려하였다. 그 결과, VC의 발행자 및 내용이 변조되지 않았는지 확인할 수 있으며 기술적으로 구현 가능하다는 것을 확인할 수 있었다.

### 7.13. 대일본인쇄

- 속성 정보 기법: 속성 정보의 증명 방법으로 DID/VC를 사용한다.
- 본인 확인, 실재 증명 방법: 정보 없음

## 8. Trusted Web 지갑 구현, 블록체인 활용

### 8.1. DataSign

- 지갑 구현 상세: 구현함. metamask/eth-hd-keyring을 키 관리에 사용한 크롬 확장 프로그램을 통해 DID 관리를 수행한다.
- 블록체인, 분산원장 활용: ION/Bitcoin

### 8.2. NRI 디지털

- o 지갑 구현 상세: 구현함. 스마트폰 기반, NRI Digital이 보유한 것을 활용. VC를 관리하고, 암호 키 관리는 백업 서비스로 사업자에 의한 계정 관리를 한다.
- o 블록체인, 분산원장 활용: ION/Bitcoin

### 8.3. 동경대학교

- o 지갑 구현 상세: 구현함. PLR 앱을 지갑이라고 칭하며, 학습자의 VC, 암호키관리, VP를 생성 및 공개하였다.
- o 블록체인, 분산원장 활용: 정보 없음. DID는 Verifiable Data Registry (MySQL)에 등록한다.

### 8.4. 후지쓰 일본

- o 지갑 구현 상세: 구현함. IDYX 내의 스토리지(월렛)에서 속성 증명서(VC)를 관리한다.
- o 블록체인, 분산원장 활용: 정보 없음. DID는 IDYX의 공통 원장에 등록한다.

### 8.5. 시믹

- o 지갑 구현 상세: 구현 가능. 병원 직원 앱, 제약회사/CRO 직원 앱으로 지갑 구현이 가능하다. 교환 가능한 엔티티 조합은 Trusted Directory: Azure Server에 저장되며, 데이터 교환은 클라우드 스토리지: BOX를 사용한다.
- o 블록체인, 분산원장 활용: Keychain Core/Bitcoin

### 8.6. ORPHE

- o 지갑 구현 상세: 구현함. DataGateway의 Woollet을 기반으로 지갑 앱을 구현하고 있으며, VC 관리 (Hyperledger Aries 기반)에 추가하여 암호 키 관리를 구현할 예정이다.
- o 블록체인, 분산원장 활용: Woollet 블록체인 네트워크(Hyperledger Indy). 토큰 등록에는 AstarNetwork를 사용한다.

### 8.7. DataGateway



- o 지갑 구현 상세: 구현함. 로컬 지갑(Woollet)에서 VC 관리한다.
- o 블록체인, 분산원장 활용: Woollet 블록체인 네트워크(Hyperledger Indy)

#### 8.8. 안마

- o 지갑 구현 상세: 구현함. 각 엔티티의 기기 (월렛애플리케이션)의 저장소에서 DID 및 암호화 키를 관리한다.
- o 블록체인, 분산원장 활용: Keychain Core / Bitcoin

#### 8.9. Alaxala Networks

- o 지갑 구현 상세: 구현함. Quorum에 액세스하는 노드(엔티티)에 대해 지갑을 생성한다.
- o 블록체인, 분산원장 활용: Quorum. 비공개 요구 사항에 대한 준수, 노드 간 협상 기능을 갖추고 있다.

#### 8.10. 도시바테크

- o 지갑 구현 상세: 정보 없음. 통신 노드는 CG EDGE, DG HUB가 담당한다.
- o 블록체인, 분산원장 활용: ION/Bitcoin

#### 8.11. JISA

- o 지갑 구현 상세: 구현함. VC 및 암호 키는 월렛 애플리케이션(Node.js)에서 관리한다.
- o 블록체인, 분산원장 활용: ION

#### 8.12. 텐쓰

- o 지갑 구현 상세: 구현하지 않음. X25519 등의 키 합의(키 공유)에 대한 지원이 없기 때문에 지갑은 구현하지 않도록 설계하였다. 비밀 키 관리는 로컬 스토리지에서 수행된다.

- o 블록체인, 분산원장 활용: Algorand

### 8.13. 대일본인쇄

- o 지갑 구현 상세: 구현함. 지갑(Hyperledger Aries 기반)에서 VC와 암호화 키를 보관한다.
- o 블록체인, 분산원장 활용: Hyperledger Indy. DID와 관련된 VC에 대한 데이터가 식별 될 가능성이 있어 개인정보보호 위험이 높아지는 우려가 있으므로 분산 원장 등에서 공개되지 않는 하이퍼레저 인디를참조하고 있다.

## 9. Trusted Web 구현 세부사항 요약

### 9.1. 데이터 제어 거버넌스 아이디어

- o 실험에서 13개 기업 중 8개 기업이 개인 또는 법인에 의해 데이터를 분산 관리하는 형태를 채택하였다. 일부 기업은 암호화 키의 복구를 위해 백업 스토리지를 설치하고, 제 3자(스토리지 관리자)에 의존하는 패턴이나, 데이터 이용을 위해 서비스 업체가 데이터 홀더의 동의에 기반하여 교환하는 데이터를 로그로 관리하는 패턴 등을 사용하였다.
- o 분산 관리를 위해서는 여러 장치에서 관리되는 데이터의 완전한 동기화를 보장하기 위한 설계 및 구현 비용이 많이 들며, 특히 개인이 관리하는 분산 관리된 데이터를 관리하는 데는 예전보다 리스크와 부담이 커졌다. 개인정보나 암호화 키와 같은 보안적인 관리가 필요한 경우에는, 개인이 관리를 맡는 것은 큰 리스크이며, 데이터 컨트롤러 능력을 개인에게 부여하는 것의 가치와 균형을 경제성 및 운용성의 관점도 고려하여 정확하게 평가해야 한다.
- o 일부 기업에서는 데이터를 중앙집중적으로 관리하는 것에 대한 도전 필요성을 느끼지 않는다는 의견도 있다. Trusted Web에서는 데이터 컨트롤러 능력을 기능요소 중 하나로 제시하고 있으나, 데이터 컨트롤러 능력에 대한 Trusted Web 구상으로서의 스탠스를 명확하게 기업에게 보여주는 것이, 이후의 구현을 기업이 맡게 되는 것을 고려하면 유익하다.
- o 데이터의 검증성과 트러스트를 보장하기 위해, 법 규제 등에 의한 거버넌스의 필요성을 제시하는 기업이 있으며, 그 중에는 공통 트러스트 프레임워크의 필요성을 언급하는 기업도 있다. 이번 프로토타입 시스템에서는 데이터나 시스템에 대

한 거버넌스 전제에 대해서는 모든 기업에서 명확하게 설정하지 않았으나, 일부 기업에서는 물리적인 계약으로 서비스 이용에 대한 거버넌스(예: 데이터 처리에 관한 합의, 데이터 접근 권한 등)를 추구하는 것으로 알려져 있다.

- 이후 서비스로 구현해 나가는 데 있어서는 “거버넌스를 어떻게 보장할 것인가“, “어느 정도 거버넌스에 의해 통제를 할 것인가“에 대해서는 언젠가 상세한 검토가 필요할 것이다. 또한 기업 측에서는 어떤 내용을 거버넌스로 보장해 나가야 하는지, 그리고 그 거버넌스 룰의 안을 구체적으로 보여주는 것이 이후 검토를 유익하게 진행하기 위하여 중요하다.

## 9.2. 합의 형성 및 추적의 사고 방식

- 합의 형성에 관여하는 주체(합의의 범위)로는 대부분의 사업자가 사업 스키마에 등장하는 스테이크 홀더의 범위 내에 머무르고 있으며, 서비스 시스템에서 예상하지 않은 제 3자를 포함한 합의 형성(예를 들어, 데이터 홀더의 데이터 공유 대상에서 더 이상의 제 3자에게 데이터 공유되는 경우, 데이터 홀더의 합의에 기반하여 공유되는 체계)까지 커밋하고 있는 사업자는 확인할 수 없었다.
- 기술적으로 과제가 있는 것도 고려되지만, 어차피 서비스의 범위로는 제3자에게 데이터 공유를 고려하지 않았기 때문이라고 생각된다. 반면, 이후 사회 실현 및 횡적 전개를 고려한 시장 확대를 생각할 때, 데이터의 이용 범위를 확대하려는 움직임은 기본 구상 내에 있다고 가정되므로, 제 3자를 포함한 합의 형성의 실현을 위한 방법을 정리하는 것은 이후의 구현성을 높이는 데 유용하다고 생각한다.
- 합의의 취소에 대해서는 대부분의 사업자가 기술적으로는 가능하였다(스마트 계약을 사용하는 경우와 합의의 취소에 관한 합의를 UI에 구현하는 패턴이 있었다). 반면, 몇몇 사업자는 합의의 취소를 구현할 필요가 없다고 하였다. 데이터의 내용에 대해 합의를 이루고 있는 사업자에 대해서는, 합의를 취소하더라도 데이터가 공유된 사실은 변하지 않으며, 또한 폐기를 요청하더라도 실제로 폐기된 것을 엄밀히 확인할 방법은 없기 때문에 구현할 필요가 없다고 하였다.
- 추적의 대상으로는 합의한 사실의 추적(합의 기록을 UI 상에서 확인하는 케이스)과 합의 기록에 추가로 교환한 메시지의 내용까지 추적하는 케이스가 관찰되었다. 본 사업 내에서 가정하는 추적은, 동일 서비스 시스템 내의 스테이크 홀더가, 자신의 교환 기록을 후에 확인할 수 있는 것을 지칭하는 것이 주로이며, 일종의 데이터 추적 가능성으로 보장되는 데이터의 제3자 이용의 추적 및 이용 방지까지 커밋한 케이스는 관찰되지 않았다.

- 보다 실용적인 서비스를 생각할 때 제3자까지 포함된 데이터 추적 가능성이 보장된 시스템의 구현을 목표로 해야하는것이 중요하다고 생각하지만, 구현 비용이나 그것을 필요로 하는 유스케이스의 수를 고려할 때, Trusted Web 구상에서 얼마나 시간을 할애하여 검토할지는 협의가 필요하다고 생각된다.

### 9.3. 속성 정보 인증 방법

- 실증 사업에서는 모든 사업자가 DID를 채택하였으며, 13개 사업자 중 11개 사업자가 DID와 VC의 조합을 속성 정보 인증의 구조로 채택하였다.
- 실증 사업에서는 VC의 채택에 있어서, 다른 방법과 비교 평가를 한 후 채택한 경우는 없으며, 다음 해의 실증 사업에서는 다른 방법의 평가 또는 비교 검토를 하여 왜 그 기술을 채택하게 되었는지를 명확히 하는 것이 중요하다.

### 9.4. 본인 확인 및 실재 증명 방법

- 본인 확인 및 실재성 증명의 구현에 있어서는 Azure AD의 인증 기능을 사용하는 경우나 스마트폰의 생체 인증을 사용하는 경우가 있는 반면, 대면으로 확인을 전제로 프로토타입 시스템의 구축을 진행한 사업자도 있었다.
- 일부 사업자들은 G-Biz ID의 채용 가능성에 대해 언급하며, 앞으로의 연계가 예상된다.
- 메타버스 공간에서 인증 서비스의 유스케이스에 대해 다른 사업자들은, 몰입감을 유지한 본인 확인의 필요성을 과제로 제기하고, 유스케이스의 내용에 따라 본인 확인에 요구되는 요건의 차이가 있음을 다시 한 번 확인할 수 있었다.

### 9.5. 지갑 구현, 블록체인 활용

- 13개 사업자 중 11개 사업자가 월렛사용에 대해 언급하였으며, 월렛의기능으로는 속성 증명 (VC 등)이나 암호 키를 관리하는 통신 노드로서 위치되는 경우가 대부분이었다.
- 본 실증 사업에서는 월렛의 정의에 대해 명확하게 나타내지 않았으며, 유스케이스의실현에 필요한 기능을 바텀업으로 사업자에게 구축을 요구하고, 구축된 시스템에 대해 월렛의 사용 여부를 확인하는 형태로 월렛의 기능 범위를 확인하였다.
- 각 사업자 모두 월렛에 대해 명확한 정의를 제시하지 않으나, 대부분의 사업자는

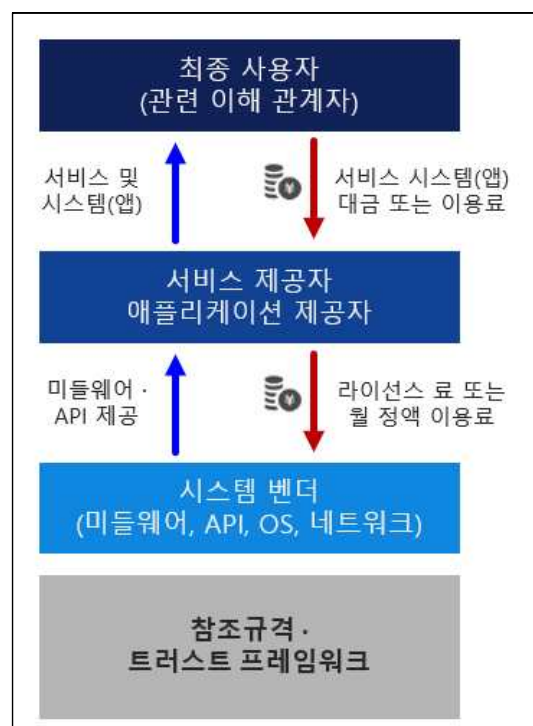
VC나 암호 키를 관리하는 디바이스, 데이터 통신을 위한 에이전트로서 월렛을 활용하고 있다.

- o 이번에는 모든 사업자가 DID를 채택하였기 때문에, DID의 등록 기반으로 블록체  
인/분산 원장 또는 VDR(Verifiable Data Registry)을 활용하고 있다.
- o 이번 사업에서는 비트코인 기반의 퍼블릭 체인을 사용하는 사업자가 비교적 많았  
지만, ALAXALA Networks, 대일본인쇄, DataGateway 등은 퍼미션형(프라이빗  
형) Quorum이나 Hyperledger Indy를 각각 채택하여, 앞으로 실증 사업을 진행  
할 경우, 그 메리트·디메리트(명의 인증의 위험, 구현 비용 등)를 정리해 나가는  
것이, 다른 사업자를 포함하여, 시스템의 설계를 검토하는 데 유용하다.

## 10. Trusted Web 비즈니스 모델

비즈니스 주체는 최종 사용자, 서비스 제공자, 시스템 벤더로 구분할 수 있다. 시스템 벤더는 미들웨어와 API를 서비스 제공자에 제공하고 서비스 및 시스템(앱)을 최종 사용자에게 제공한다. 최종 사용자는 서비스 제공자에게 서비스 시스템(앱) 이용료를 지불하고 서비스 제공자는 시스템 벤더에게 라이선스료 또는 월 정액이용료를 지불한다. 이러한 모델은 W3C, DIF, ISO/IEC, ODF, GAIN, OIX등의 규격을 참조한다.

다음 그림은 Trusted Web의 비즈니스 모델을 보여준다.



## 10.1. 비즈니스 주체

### o 최종사용자(관련 이해 관계자)

- MFP 사용자, 메타버스 사용자, 환자, 의료기관, 연구기관, 학생, 대학, 사용기업, 증명서 발행단체, 중소기업, 보조금 사무국, 단소배출량 공개 기업
- 설비메이커, 중소기업자, 보조금 사무국, 제품사용자, 병원, 병원스텝, 제약기업 /CRO 스태프
- 웹사이트 열람자, 사이트 운영 사업자, 애드테크사용자

### o 서비스 제공자, 애플리케이션 제공자

- 도시바테크(MFP 메이커), KDDI(가상공간제공), ORPHE, JISA, 얀마, 시믹, 텐츠, 대일본인쇄(공조앱벤더), Trusted Network Provider(공익적 제3자: IPA 등)

### o 시스템 벤더(미들웨어, API, OS, 네트워크)

- CollaboGateJapan, Keychain, BlockBase, 이토 타다 테크노 솔루션, Cyaltrust, 알렉사라네트웍스, ISID, 동경대학교, 야후
- DataSign, DataGateway, NRI 디지털, 후지쓰 일본

### o 참조규격, 트러스트 프레임워크

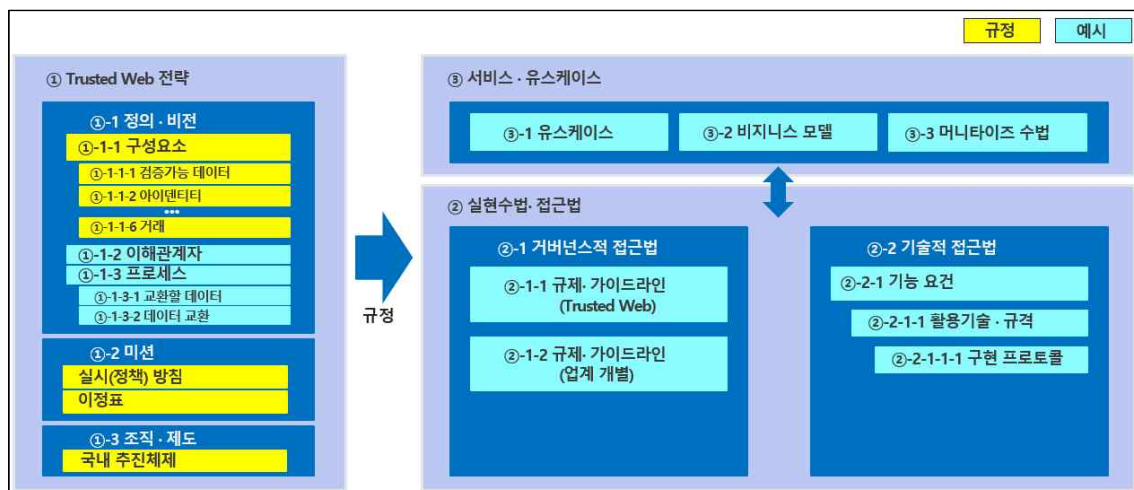
- Verifiable Credentials Data Model v1.1 (W3C)
- VC Implementation Guidelines (W3C)
- Decentralized Identifiers (DIDs) v1.0 (W3C)
- DIDComm Messaging v2.0 (DIF)
- Sidetreev1.0.0 (DIF)
- Well Known DID Configuration (DIF)
- ISO/IEC 18033 (ISO/IEC)
- OpenID for VC Issuance (OIDF)
- OpenID for VP (OIDF)
- SIOP v2 (OIDF)
- GAIN Trust Framework (GAIN)
- OIX Guide to Trust Frameworks for Smart Digital Identity (OIX)

## 10.2. 비즈니스 모델

- 각 Use Case에 따라 참여하는 이해 관계자 수와 유형, 수익 창출 방법은 다르지만, Trusted Web과 관련된 서비스와 애플리케이션을 상품으로 사용하여 서비스 제공 업체 및 애플리케이션 제공 업체가 직접 또는 국가, 지방자치단체 등의 이해 관계자를 통해 간접적으로 최종 사용자에게 가치를 제공하는 형태로 비즈니스 모델을 구축하고 있다.
- 서비스 또는 애플리케이션 구현 시, 시스템 벤더가 중심이 되어 미들웨어 및 API를 라이선스 판매하는 패턴이나 구독 형태로 제공하는 패턴이 수익 창출 방법으로 고려된다.
- Trusted Web의 구현을 위해서는 서비스 제공 업체와 시스템 벤더의 역량이 필수적이며, 분야 및 산업의 관점을 고려한 플레이어 맵의 세분화와 매칭을 촉진하는 커뮤니티 형성이 효과적이다.
- 참여기관 중 최종 사용자를 포함하여 구현한 사례는 거의 없었다. Trusted Web의 가치를 사회에 알리기 위해서는 사용자 층의 참여를 유도한 후 사용자가 효과 및 가치를 계산하는 것을 포함하는 실증 사업을 실행하는 것이 효과적이다.

## 11. Trusted Web의 전체 이미지

Trusted Web 전략, 서비스·유스케이스, 실현수법·접근법으로 구분할 수 있다. 다음 그림은 Trusted Web의 규정 및 예시이다.



## 11.1. Trusted Web 전략

### o ①-1 (정의 및 비전 일반) (규정)

- “검증 가능성“의 정의 및 생각의 명확화
- Trust의 대상 및 내용의 명확화
- 용어의 정의의 명확화, 쉬운 표현으로의 재검토
- 구현 프로토콜에 대한 위치 표현에 대해
- 논의하는 데 필요한 전제의 제외 (재설정)의 필요성
- Trusted Web에서 충족해야 하는 요건의 명확화
- Trusted Web에 따른 메리트 / 효과 / 디메리트/ 리스크 구체화
- 보안 / 프라이버시를 포함한 목표로 하는 모습의 명확화
- 물체를 엔티티로 한 경우의 요건 (목표하는 모습)의 설정

### o ①-1-1 (구성 요소) (규정)

- 구성 요소의 정의의 명확화
- 개인 데이터를 다룰 경우의 구성 요소 (아키텍처)의 생각
- Identity를 사용하는 경우의 다루기 / 생각
- 트랜스포트 프로토콜의 선택 기준
- VC 형식이나 속성 이름의 정의의 필요성
- 물체의 Identity 처리에 대한 생각
- Identity 그래프의 활용 장면 / 방법의 정의
- Wallet을 공동으로 사용할 때의 권한에 대해
- 교환되는 데이터의 정의 / 표준화
- VC (검증 가능한 데이터)의 유효 기간에 대해

### o ①-1-2 (이해관계자) (예시)

- 개인 데이터를 다룰 경우의 Issuer 요건
- Trusted Web을 평가하는 주체 / 체제

### o ①-1-3 (프로세스) (예시)

- 자기 주권형 데이터 관리/제어의 실현 방법
- 프로세스 (합의 이행의 추적)의 정의/생각의 명확화
- 합의 이행의 추적에서의 데이터 추적성 고려



- 개인 데이터의 보관 규칙의 생각/규정에 대해
- 암호 키 관리에 관한 가이드라인의 명시적 필요성
- 암호 키 관리에 대한 과제
- Trusted Web에서 KYC의 위치 표현, 생각
- KYC의 실현 방법에 대해
- Wallet 간 상호작용, Wallet 및 Wallet 사용자의 신뢰성 보장에 대해
- 당사자 인증의 신뢰성 강도의 생각, 방법에 대해

#### o ①-2 (미션) (규정)

- Trusted Web SDK의 개발 / 보급을 위한 노력
- 일반 사용자 / 기업을 대상으로 한 PR 콘텐츠의 제작
- Trusted Web의 국제적인 합의를 위한 로드맵
- 일반 소비자에 대한 리스크 (정보 유출, 위장 등)의 알림

#### o ①-3 (조직/제도) (규정)

- Trusted Web의 추진과 관련된 국가의 참여의 필요성
- Trusted Web의 오픈 커뮤니티의 구성
- Identity를 사용하는 경우의 다루기/생각

### 11.2. 실현수법 · 접근법

Trusted Web의 요구 사항에 대한 구현 방법 · 접근 방식을 정리하였다. 구현 방법 · 정책에 대한 WP의 기술적 상세성 · 강제력을 보여준다. 데이터의 특성에 대응한 신뢰성 보장 수단을 선택한다. 특정 커뮤니티에서 데이터, 데이터 교환의 신뢰성을 보장하는 방법을 나타낸다. 수익성을 고려한 구현 방법 검토와 Wallet을 분실한 경우의 복구 방법을 보여준다.

#### o ②-1 (거버넌스적접근법 - Trusted Web 내부) (예시)

- Issuer(데이터 발행자)의 신뢰성 보장 수단
- 합의이행 범위 이외에서의 데이터 이용 추적(제한 · 제어)을 위한 견제성의 필요성
- 업계협단의 일본 버전 Trust Framework 작성
- Trusted Web(분산 ID)에서 개인정보 보호에 관한 규정의 필요성
- 사용자에게 의한 비밀키 관리를 규정하는 규칙 검토(견제성-업계 개별)
- 헬스케어 데이터의 신뢰성 보장 기구의 표준화, 가이드라인의 제정

- 일반 사용자 · 기업을 위한 PR 콘텐츠 제작

#### o ②-2 (기술적 접근법) (예시)

- 자기 주권형 데이터 관리 · 제어의 실현 방법
- 공개키를 획득할 수 없는 경우의 데이터 검증 방법
- Trusted Web의 구현 방법에 관한 구체적인 규정의 필요성
- KYC의 실현 방법
- UI/UX를 고려한 애플리케이션 기능, Wallet 기능의 생각
- UI/UX에 관한 기능 · 비기능 요구사항의 생각
- UI/UX의 요구사항에 대해
- 블록체인의 이용에 관한 보안 요구사항 설정

### 11.3. ③ 서비스 · 유스케이스 (예시)

- o Trusted Web에서 비즈니스 모델 실현에 대하여
- o 비즈니스 모델 실현을 위한 인센티브 설계의 필요성
- o 헬스케어 데이터의 유스케이스에서 데이터 컨트롤의 요건 적용 여부에 대하여
- o Trusted Web 시스템 구축, 서비스 제공 실현에 관한 추진체제

## 12. Trusted Web의 전략

### 12.1. Trusted Web의 내용 명확화

Trusted Web의 6가지 구성 요소에 대해 “이해하기 어렵다“, “정의를 명확하게 해야한다“는 의견이 제기되었다. 구체적으로 “데이터 교환 기록이 트랜잭션 및 노드 각각에서 정의되어 있기 때문에 구성 요소마다 역할의 차이를 명확히하는 것이 필요하지 않을까“, “유스케이스의 내용(물건의 신원이나 개인 데이터를 다루는 경우 등)에 따라 패턴이 있으면 좋겠다“는 것도 제기되어 아키텍처의 재구성 및 재검토의 필요성이 제기되고 있다.

### 12.2. 합의, 추적 정의, 생각 방식의 명확화

합의에 대해서는 데이터의 내용 뿐만 아니라 제시, 공개 등의 데이터 교환에 대해서도 합의를 이루고 있는 사업자도 있으며, 또한 추적에 대해서도 합의의 이행에 대한 추적(확인, 열람)으로 정의한 사업자도 있고, 데이터의 유통에 관한 추적(일명 데이터 추적성)을 염두에 둔 검토를 진행하고 있었던 사업자도 있었다. 합의 및 추적의 생

각 방식을 포함하여 Trusted Web에서 추구하는 내용을 명확히 나타내면, 사업자가 서비스나 시스템을 검토할 때 Trusted Web을 참조하는 기회가 늘어날 것으로 생각된다.

#### 12.3. 인증서 발급자(Issuer)의 신뢰성을 확보하고 평가하는 체계의 규정

Trusted Web에 등장할 수 있는 이해관계자에 관한 논점으로, Issuer의 요건이나 Issuer의 신뢰성을 평가하는 체계의 구현을 기대하는 의견이 많았다. Issuer는 속성 정보를 증명하는 주체이며, 서비스 및 시스템 전체의 신뢰성을 보장하는 데 중요한 위치(신뢰의 근간을 담당하는 주체)에 있기 때문에, 개별 요건이나 그를 평가하는 체계를 어떻게 할 것인지, 백서에서 언급해야 한다.

#### 12.4. Trusted Web의 조직 및 추진 체계

유스케이스 중에는 산업으로서의 디지털화를 추진하는 데 있어서 민간 사업자의 노력만으로는 조정이 어렵고, 디지털화를 추진하기 위한 법령의 정비, 비용 부담 등도 포함한 국가적인 탑다운으로의 정책 실행 등, 행정과 민간이 일체화된 추진 체제 구축이 중요하다는 의견이 제기되었다. 현재는 기업마다 Trusted Web의 사회적 구현을 위한 움직임이 개별적으로 이루어지고 있는 것을 받아서, 다양한 기업이 의견 교환을 할 수 있는 오픈 커뮤니티를 구성하여 서로 운용성을 고려한 구상을 진행하는 방향성에 대한 의견이 있다. 이러한 의견을 바탕으로, 이후 정부의 관여 범위나 국내 구체적인 추진 체제에 대해 검토하고, 백서에서 보여줄 필요가 있다.

#### 12.5. 아키텍처 6 구성요소 재구성 및 재설계 방향

Trusted Web의 아키텍처(6 구성 요소)에 대해 이해하기 어렵다는 의견이 있어 아키텍처를 개선하기 위해 시범 기간 동안 사업자 주도로 유스케이스 내용을 6 구성 요소에 적용하는 작업을 수행했지만, 그 과정에서도 적용에 어려움이 있었다. 그 이유로는 정의가 명확하게 정해지지 않았거나 유스케이스의 종류에 따라 적용하는 것이 어려운 경우가 있기 때문이다. 위에 더해 6 구성 요소가 처음에 (백서 1.0에서) 설정되었던 4 기능을 재정리한 것으로, 각 요소에 Trusted Web의 기능적 특징을 가지려는 사업자의 고민이 있었을 가능성이 있고, 그로 인해 적용이 더욱 어려워졌을 수 있다. 실제로는 구성 요소와 기능은 반드시 관련된 것은 아니며, “검증 가능한 영역을 확대하여 신뢰성을 향상시키는” 등 Trusted Web이 추구하는 모습을 실현하려 할 때, 유스케이스별 전체에 의존하지 않는 프리미티브한 구조가 6 구성 요소이다. 따라서 사업자에게는 6 구성 요소를 고수할 필요가 없으며, 또한 검토한 시스템 구성이 반드시

6 구성 요소에 적합한 것은 아니며, 더 나아가 각 요소별로 Trusted Web에 특징적인 관점이 포함되지 않을 수도 있다는 것 등을 사전에 알려야 한다.

### 13. Trusted Web의 접근 방법

#### 13.1. Trusted Web을 실현하기 위한 거버넌스에 대해

기술과 거버넌스로 커버되는 영역을 명확히 분리하도록 요구하는 의견도 있다. 구체적으로 거버넌스에 의해 보장되어야 할 내용, 시스템으로는 발행자의 신뢰도를 TrustGraph등을 통해 측정하는 방법이나, 데이터의 복사 등으로 추적할 수 없는 범위를 법제도로 보장하는 등 데이터 거버넌스적인 시각에서 여러 의견이 있다. 이러한 과제 제기에 대해 정부나 Trusted Web 추진 협의회 등이 대답을 가지고 있는 것은 아니며, 사업자들은 문제의식뿐만 아니라 구체적인 해결책을 제시해주길 원하므로 이를 명확히 밝히는 것이 필요하다. 사업자들의 의견과 같이, 데이터 복사 또는 다운로드 제한 등 기술적으로 보장할 수 없는 영역에서 트러스트와 검증성을 보장하기 위해서는 법제도를 포함한 거버넌스로 규정해야 한다. 반면, 거버넌스로는 보장할 수 없는 그 영역에서 정말로 트러스트를 보장해야 할 필요가 있는지에 대해서는 논의가 필요하다. 특히 거버넌스의 설정과 자유로운 데이터 활용은 트레이드오프의 관계가 되는 경우가 많아, 데이터 활용보다 트러스트가 우선되는 것은 일차적인 시각일 뿐이므로, 윤리적인 측면, 기술적인 측면, 사업적인 측면 등 다양한 시각에서 의욕이 있는 사업자들이 중심이 되어 업계를 가로지르는 관련 이해관계자를 모아 논의해야 할 내용이다.

#### 13.2. 암호 키 관리 방법에 대해

암호 키를 관리하는 방법을 논의할 필요성이 제기되고 있다. 이번 유스케이스에서는 암호 키(비밀 키)를 이용한 전자 서명의 검증에 따른 검증성, 트러스트를 보장하는 것을 전제로 하고 있어, 전자 서명에서 암호화를 담당하는 비밀 키를 안전하게 관리하는 것은 Trusted Web에서 제공하는 트러스트의 가치를 보장하고 있다. 가령 암호 키가 유출된 경우, 본인 이외에도 서명하여 데이터를 전송할 수 있게 되므로, 위조나 변경이 유행될 가능성이 있으며, 분실한 경우, 재발행이 불가능하고, 이전에 보유한 데이터를 사용할 수 없게 되는 위험도 예상된다. 반면, 데이터 컨트롤러빌리티를 보장하기 위해 이 사업에서 구축한 시스템의 대부분은 분산형을 추구하고 있어, 키를 관리하는 위험을 개인에게 분담시키거나, 일부분은 집중적인 구조로 키의 관리를 제 3자에게 위임하는 등을 논점으로 검토한 사업자도 있다. 암호 키를 분실한 경우의 위

협과 키를 관리할 수 있는 능력을 감안하여, 특정 조직이 집중적으로 키를 관리하는 선택지를 채택하는 것이 현실적으로 가능하므로 데이터 컨트롤러빌리티나 분산적인 사상을 Trusted Web 구상의 어떤 위치에 놓을 것인지(전제로 할 것인지, 선택적으로 할 것인지) 명확히 밝혀야 한다.

### 13.3. 비즈니스 모델 구현에 대한 과제

비즈니스 모델 구현(비용 및 수익 모델의 성립)을 위해서는, 발행자가 디지털 상에서 증명서를 발급하는 인센티브를 확보하는 체계에 대한 과제가 제시된다. 발행자는 증명서를 데이터 홀더에게 발급한 후에도, 해당 증명서는 이후에 또는 유효기간을 설정하지 않은 경우, 갱신 내용이 없는 경우 데이터 홀더가 영구적으로 재사용할 수 있는 경우도 있다. 발행자가 증명서의 유효기간을 설정하는 경우, 갱신 내용이 있는 경우에는 재발행이 발생된다. 이 경우, 초기 발행 시에는 발행 수수료 형태로 데이터 홀더가 발행자에게 비용을 지불할 수 있을 것으로 예상되지만, 그 이후의 지속 가능성을 고려할 때, 비즈니스 모델이 실제로 성립하는지가 과제이다. 그리고 그 경우에, 시스템의 이용료는 누가 부담하는 형태로 성립될 수 있는지, 사업자로부터 현실성 있는 아이디어와 검증이 요구된다. 본 실증 사업은 “개발 실증”이며, 엔드 유저나 특정 발행자의 참여는 가정하고 실행되는 경우가 대부분이지만, 다음 해부터의 실증 사업에서는 참여하는 스테이크 홀더를 확대하고, 수익 모델 평가를 포함한 “과제 해결 실증”의 설계를 통해 보다 구체적인 구현 가능성을 검증할 수 있다.

## 14. Trusted Web의 참여자 및 요구사항

### 14.1. 사용자(어플리케이션)

개인 데이터(ID, 정보)를 생성하고, DID에 연결한다. 사용자는 자신과 관련된 데이터를 제어할 수 있다. 전송데이터를 보호할 수 있는 안전한 채널을 이용한다.

### 14.2. 신원정보 발급 기관

신원정보를 보유하고 있는 기관·기업(여권정보, 운전면허 정보, 학위정보, 사원정보, 신용 정보 등)으로 디지털 신원정보(VC, Verifiable Credential)를 생성하고 VC로 부터 VP(Verifiable Presentation)를 생성할 수 있다.

### 14.3. 검증기관

정보 수신자, 데이터 이용기관·기업으로 사용자로부터 VC를 전달받아 발급기관에

검증 요청을 한다. VP를 통해 사용자를 검증할 수 있다.

#### 14.4. 플랫폼(인터넷 서비스)

개인 데이터 활용 측면에서 검증기관과 분리되며 고객 VC 검증으로 회원 가입 (통합인증)을 수용한다. 최소 개인정보 요구 및 고객정보의 저장을 최소화 한다. 가입 · 탈퇴의 자유로움을 보장한다.

#### 14.5. 데이터 저장소

개인정보 저장을 위탁 받은 데이터 보관 · 관리기관으로 분산형 파일시스템(IPFS, InterPlanetary File System)을 이용한다. 신원정보 거래 및 데이터 전송 이력 관리를 블록체인, 노스트르 등 선택적 기술을 사용하여 수행한다. 개인의 선택에 따라 데이터 저장소를 선택할 수 있다.