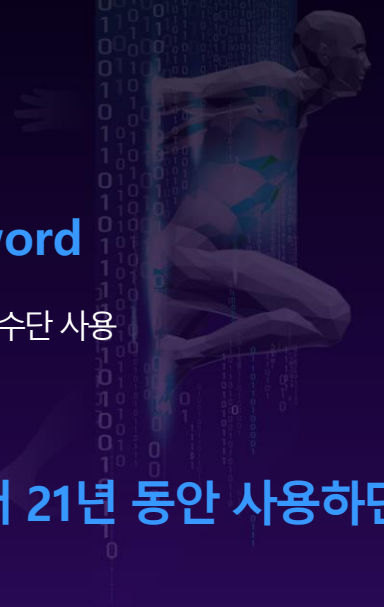
시큐업 세미나 2022
디지털 인증의 현재와 미래

THE FUTURE OF DIGITAL IDENTITY

(사)한국디지털인증협회 **이기혁 회장**

2022.10.04

디지털 인증의 변화와 혁신



✓ On-Line과 Off-Line에서 하루에 몇 번씩 본인확인하나요?

⑴ 출근할 때 사원증으로 본인 인증

⑵ 은행 Site에 접속할 때 본인 인증

⑶ 운전할 때는 운전 자격 증명 위해 운전면허증 소지

이처럼 인증을 하는 행위는 On-Line과 Off-Line에서 자주 발생

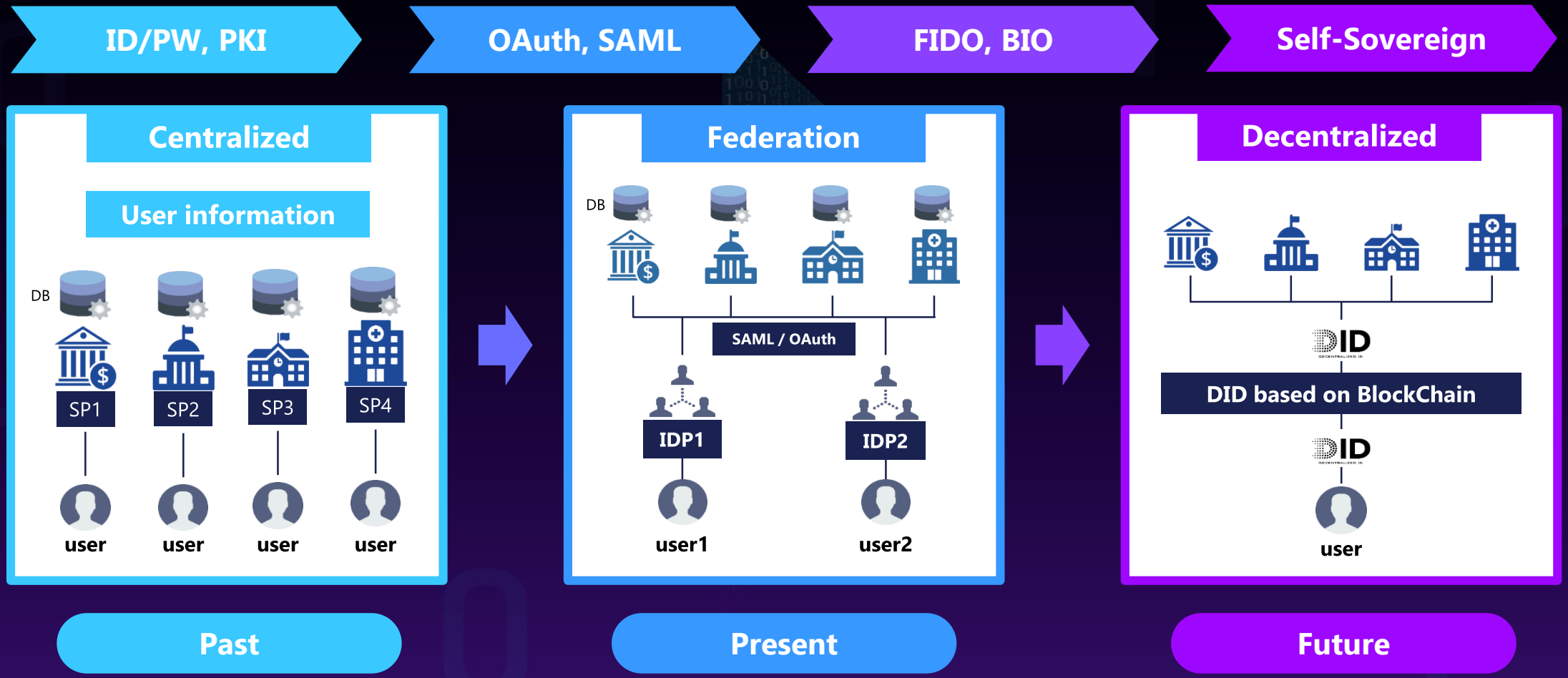
✓ 가장 간단하고 편리한 인증수단은? ID와 Password

- 보안상 취약점 때문에 OTP, Smart Card, 생체인증 등의 다양한 인증 수단 사용

✓ 공인인증제도가 2020년 12월부로 변경(폐지)되어 21년 동안 사용하던 인증시장 무한경쟁 도래

✓ 산업의 디지털 인프라 확대, 서비스 환경의 디지털화 변화로 디지털 인증은 서비스의 핵심 가치로 발전 요구됨

디지털 인증의 변화와 혁신



디지털 인증의 변화와 혁신

시기	1999	2002	2006	2010	2014	2018	2020
주요 이슈	전자서명법 제정, 공인전자서명 체계 마련 ('99.2)	인터넷뱅킹 공인인증서 사용 의무화 ('02.9)	공인인증서 사용 전면 의무화 ('06.12)	전자금융감독규정 개정을 통한 인증방법 확대 ('10.6)	공인인증서 사용 의무 폐지 이슈화 ('14.3)	공인인증서 전면 폐지 추진 ('18.3)	전자서명법 개정안 국회 본회의 통과 ('20.5)
인증 기술	비밀번호 등 지식 기반 인증 중심						
		공인인증 등 소지 기반 인증					
		인증기술 자율화		모바일 디바이스 인증			
				인증기술 다양화	생체인증 등 특성 기반 인증		
						블록체인 기반 인증	
							분산ID

출처:한국인터넷진흥원 자료 재구성

디지털 인증의 변화와 혁신

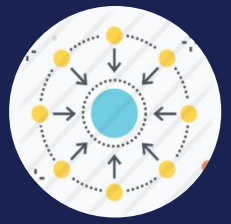
1단계 : 1990년대 말 ~ COVID 前	2단계 : COVID-19 (3년)	3단계 : COVID-19 以後
✓ 대면거래가 인터넷 기반으로 전자거래로 대체 ✓ 비대면 인증을 위한 공인인증서 등의 인증 수요가 폭발적으로 발생 ✓ 인증 사업자 확장	✓ 생활 대부분이 비대면으로 이루어지는 환경으로 도래 ✓ 새로운 간편 인증 수단, 수요 증가 계기	✓ 새로운 기술(AI, IoT, Bio, Blockchain 등)의 등장과 비대면 환경 일상화로 이용자 마인드 변화 ✓ 대면 활동들이 온라인으로 급속히 옮겨가고 ✓ 가상세계에서 콘서트, 졸업식, 선거 유세 등 사례들이 생기면서 ✓ 디지털 인증에 새로운 전환기 도래

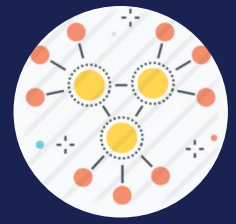
NEED FOR DIGITAL IDENTITY

사회적 필요성

ID는 동등한 인간기본권 추구를 위한
사회적 문제 해결의 시발점

보안적 필요성





안전한 개인정보관리를 위한 안전한 환경조성
보안적 필요성 대두

경제적 필요성

국가기관의 과세, 복지 등 사회적 비용 절감 및
신원확인 관련 중간사업자 배제로 이용자의 비용 절감

기술적 필요성

확장 가능한 다양한 기술(빅데이터, AI, AR, VR 등) 연계를 통해
미래 플랫폼 기반 서비스 토대 마련 필요

DIGITAL IDENTITY KEY FEATURES

간편인증
Simple Authentication

- 쉽고 안전한 FIDO 인증
- 언제, 어디서나 이용
- 서비스 확장성 보장
  (DID+ID Binding)

본인인증
Secure Identification

- 참여기관 회원 간 인증
- 대면/비대면 회원 인증
- 인증 비용 지불 주체
  → 수익 전환

자격/증명서
Credentials Verification

- 증명 가능한 정보 발급
- 온라인 자격증명 구현
- 정보 마켓 플레이스로
  자율적 생태계 구현

NFT
Non Fungible Token

- 디지털 컨텐츠 유일성 증명
- 디지털 컨텐츠 무결성 보증
- NFT 거래/유통/검증
  생태계 체인 구축

DIGITAL IDENTITY ALLIANCE MISSION

◆ Mission :

디지털 세상에서 신뢰와 책임으로 이루어진 개방형 프레임워크를 통해 인류에게 디지털 신원 제공

◆ Vision :

쉽고 간편한 신원증명으로 공공 제도, 의료 등 모든 인프라의 혜택을 누리도록 디지털 신원 인증 플랫폼을 블록체인 기반으로 통합

WELCOME TO ALL DIGITAL CERTIFICATION OFFICIALS

DIGITAL IDENTITY ALLIANCE PROMOTION TASKS

생태계 구축

생태계 중심 실증 모델 확보

기업과 기관의 디지털 인증 실증 모델 참여 기회 제공

신규 비즈니스 창출

다양한 신원정보 기반 신규사업 및 스타트업 시장진입 장벽 완화

기업/산업 간 교류 및 협력

회원사 간 정보 교환 및 네트워킹 강화

국내 • 외 세미나 및 전시회 세션 발표

기술 자문 서비스 제공

디지털 인증 기술과 시장환경 변화 대응 전문가 기술 자문

정책/제도 개선 및 전문 교육

인증 기술정책 제안 / 법률 • 제도 개선

대정부 디지털 인증 관련 정책 연구 및 제안

기술 등 전문교육 기회 제공

사업화 추진을 위한 기술 기획, 사업기획 전문 교육 제공

해외시장 개척, 글로벌화 지원

한국 및 글로벌 기술 / 서비스 표준화 추진

개별적 추진 중인 디지털 인증 기술을 표준화 추진

글로벌 인증 획득 지원(ADI Association 협력)

글로벌 서비스 제공을 위한 국제인증 획득 서비스 제공

THE FUTURE OF DIGITAL IDENTITY

- Digital Identity 보급 확산으로 정치 참여, 사회적 권리, 행복추구권을 위한 인간의 기본 권리 보장
- ID/Password 기반의 중앙 집중형 서비스 한계 극복으로 다양한 보안 문제 해결 기여
- 서비스 별 독립된 ID체계 해결로, ID 암기 등 이용자 스트레스 해소와 사회적 비용 경감
- 과도한 개인정보 제공 요청 해결 기대
- 데이터 큐레이터 사업 등 미래형 개인정보 체계 제공으로 개인정보 제공에 대한 보상 기초 마련

무한 경쟁상황에서 디지털 인증 거버넌스

- ✓ 특화된 인증 기술과 서비스로 이용기관을 확보하여 WIN-WIN 시스템 구축
- ✓ 전자서명법상의 전자서명인증사업자 인정을 받는 것이 좋은가?에 대한 자체적인 분석이 필요
- ✓ 인증 사업자(ISSUER) 측면 : 이용기관(SP) 확보가 인증 서비스 사업의 성패를 좌우하는 환경으로 변경(가입자 확대 및 수익)
- ✓ 서비스 사업자(SP) 측면 : 자체 서비스 성공 위해, 다양한 인증 서비스 적용하고 새로운 인증 서비스를 빠르게 확장하는 전략 검토
- ✓ 다수의 인증 사업자(ISSUER)와 다수의 서비스 사업자(SP)들이 손쉽게 연결 관리와 정산이 될 수 있도록 디지털 인증 생태계 거버넌스에 동참을 바랍니다

시큐업 세미나 2022

디지털 인증의 현재와 미래

Balancing Security and Privacy with Trust and Accountability

ADI Association **Ramesh Kesanupalli**

Since last we spoke

2021

- **SEPTEMBER** — Specification 1.0 Released
- **NOVEMBER** — Piloted By CVSHealth

2022

- **FEBRUARY** — Security Review Initiated
- **MARCH** — First Commercial Implementation in production from Digital Trust networks
- **APRIL** — Pilots with Hitachi
- **MAY** — ADI US Interchange launched
- **JUNE** — Specification 2.0 work started
- **AUGUST** — Joined Steering Committee of Trust Over IP
- **NOVEMBER** — ADI Korea Interchange To be launched
- **DECEMBER** — ADI Japan Interchange To be launched

Current Board member

Quick Refresh On ADI Framework

Digital Landscape : Fraud & Disinformation

Cyber Attacks & Fraud

Hackers Expose 8.4 Billion Passwords Post them Online in Possibly Largest Dump of Passwords Ever
Date: June 8, 2021

LinkedIn
Date: 2012 (and 2
Impact: 165 million user accounts
Details: As the major social network for business professionals, LinkedIn

Zynga
Date: September 2019

KYC expiration pretext used in multiple cases of online fraud
People share confidential information, OTPs and download whatever the caller asks them to without verifying. That is a problem, says police inspector Jayram Paygude of the cyber police station
PUNE Updated: Jun 25, 2020 16:35 IST

Coronavirus caused surge in online fraud, TransUnion finds

Mar
Date: 2014-18
Impact: 500 m
Details: Marric

Adobe
Date: Octobe
Impact: 153
Details: As re

Dubai police arrest In
'stars' behind Dh1.6bi
international online fi

Adult
Date: Oct
Impact: 4
Details: T

Yahoo
Date: 20
Impact:
Details:

Sina Weibo
Date: March 2020
Impact: 538 million accounts
Details: With over 500 million users, Sina Weibo is China's answer to

Equifax
Date: July 29, 2017
Impact: 147.9 million consumers
Details: Equifax, one of the largest credit bureaus in the US, said on Sept.

Imagine metaverse without absoulte identity

Disinformation & Fake News

Russia and China push 'fake news' on coronavirus crisis, report claims
EU officials claim Moscow and Beijing continue to peddle disinformation on social media and its partners.

China's disinformation threat is real. We need better defences against state-based cyber campaig
June 23, 2020 4.16pm EDT

How Russian "Fake News" Hardened America's Divide

The 10 most-viewed fake-news story on Facebook in 2019 revealed in a new report

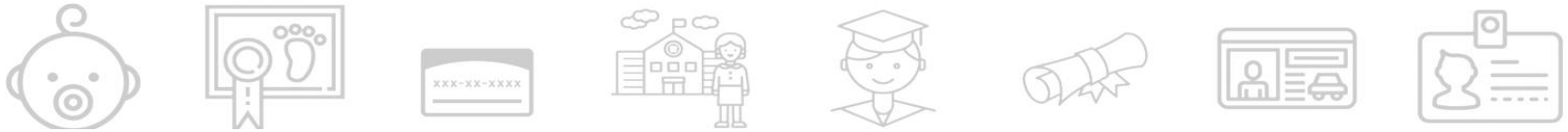
1. "Trump's grandfather was a pimp and tax evader; his father a member of
2. "Nancy Pelosi diverting Social Security money for the impeachment inquiry"
3. "AOC proposed a motorcycle ban"
4. "Trump Is Now Trying To Get Mike Pence Impeached"
5. "Ilhan Omar Holding Secret Fundraisers With Islamic Groups Tied to Terror"
6. "BREAKING: Nancy Pelosi's Son Was Exec At Gas Company That Did Business In Ukraine"
7. "Democrats Vote Now, Vote Down Vet Service"
8. "Tim Allen quote Trump's wall costs less than the Obamacare website"
9. "NYC coroner who declared the death of Jeffrey Epstein a suicide made half a million dollars a year working for the Cli
10. "Joe Biden Calls Trump Supporters 'Dregs of Society'"

Foundational needs

- Identity First – Security Model
- Existing Identity frameworks are regional – need interoperability for Global Digital Transformation
- Account Oriented Infrastructure without human binding is not suited for emerging digital world
- Establishing Accountability in the Digital world is critical
- Data representations should come from Sources for trustworthiness
- Data should not be consolidated, and should be left with issuing sources or a cloud provider for edge cases to comply with Privacy and Cross Border data regulations
- User consent is critical for any data disclosures

- **Time to change the Digital Infrastructure from an Account orientation to an Identity Orientation**

Lifecycle of Identity In Real life



The march of time

John Smith

Identity Creation

Birth Record
Identity by - Parents
Certified by - Medical Facility
Issued by - Government

Issued:
Birth Certificate
SSN
Medical Records

Student Life

Based on Birth Cert
Enrollment in Elementary
Enrollment in School
Enrollment in University

Issued:
Student ID
Progress reports
Diploma

Adult Life

Based on Birth Cert, Diploma, SSN

Created / Issued:
Employee ID
Bank Account
Automobile Title
Real Estate Title
Medical Insurance
Health Records
….

Accountability

Identity Created by Trusted People & Given to John

Owned by John
Real person behind the Identity
John responsible for that Identity

Solution

Unique Digital Address for every user

- Given by a trusted Issuer
- Bound to human attributes (Name, DOB, Country ID)
- Unlocked by FIDO authentication
- Control various Identity and Data Disclosures while interacting with Digital Services in real time directly from Issuing sources

Digital Address:

John.doe@DTX

Fix the root cause, and stop treating the symptoms

ADI Interchange architecture

Issuers

- Place of employment
- Educational institution
- Financial institution
- Driver's license issuing authority
- Passport issuing authority
- Medical facility

1 Create Digital Address

2 Issue Verifiable Credential

✓□ Easy integration for Issuer

API calls to create Verifiable Credential and publish to Digital Address

Directory Services

(multiple regional directories for users, one global directory for entities)

Issuer's agent

Digital Address Services

DLT

FIDO

Digital address app or card

User

4 Prove identity biometrically using Digital Address

5 Provide consent to share Verifiable Credential*

Service Providers

- Digital retailer
- Healthcare provider
- Pharmacy
- Travel and transportation provider
- Prospective employer
- Insurer

3 Request Verifiable Credential*

6 Validate before providing services

✓□ Easy integration for Service Provider

API calls to request and view Verifiable Credential

** Could be a particular claim instead of an entire credential*

5 Core Principles of ADIA

We Do Not Own Personal Data

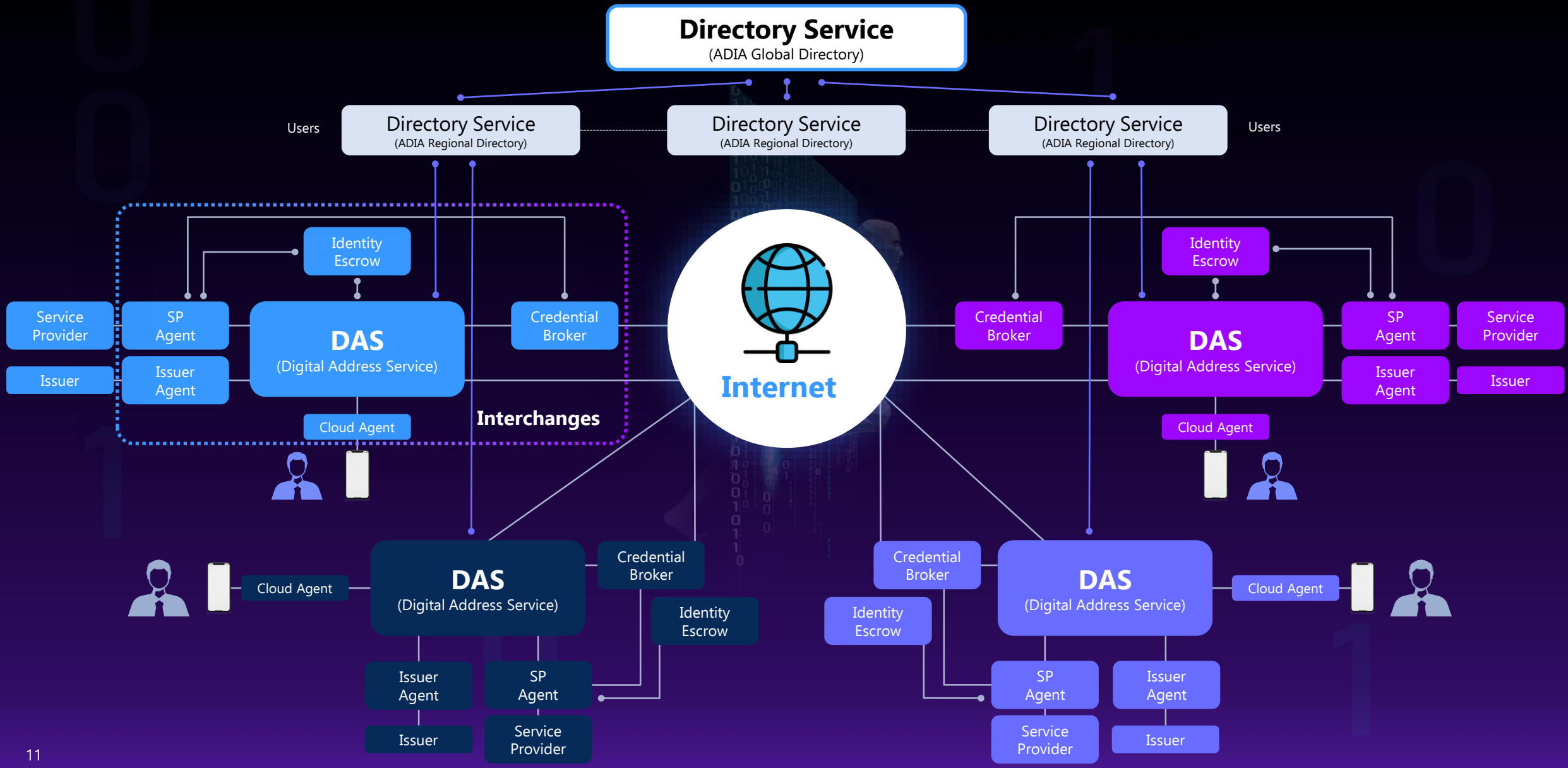
Personal ID Data Remain with Issuers Only

User's Consent for Data Disclosure

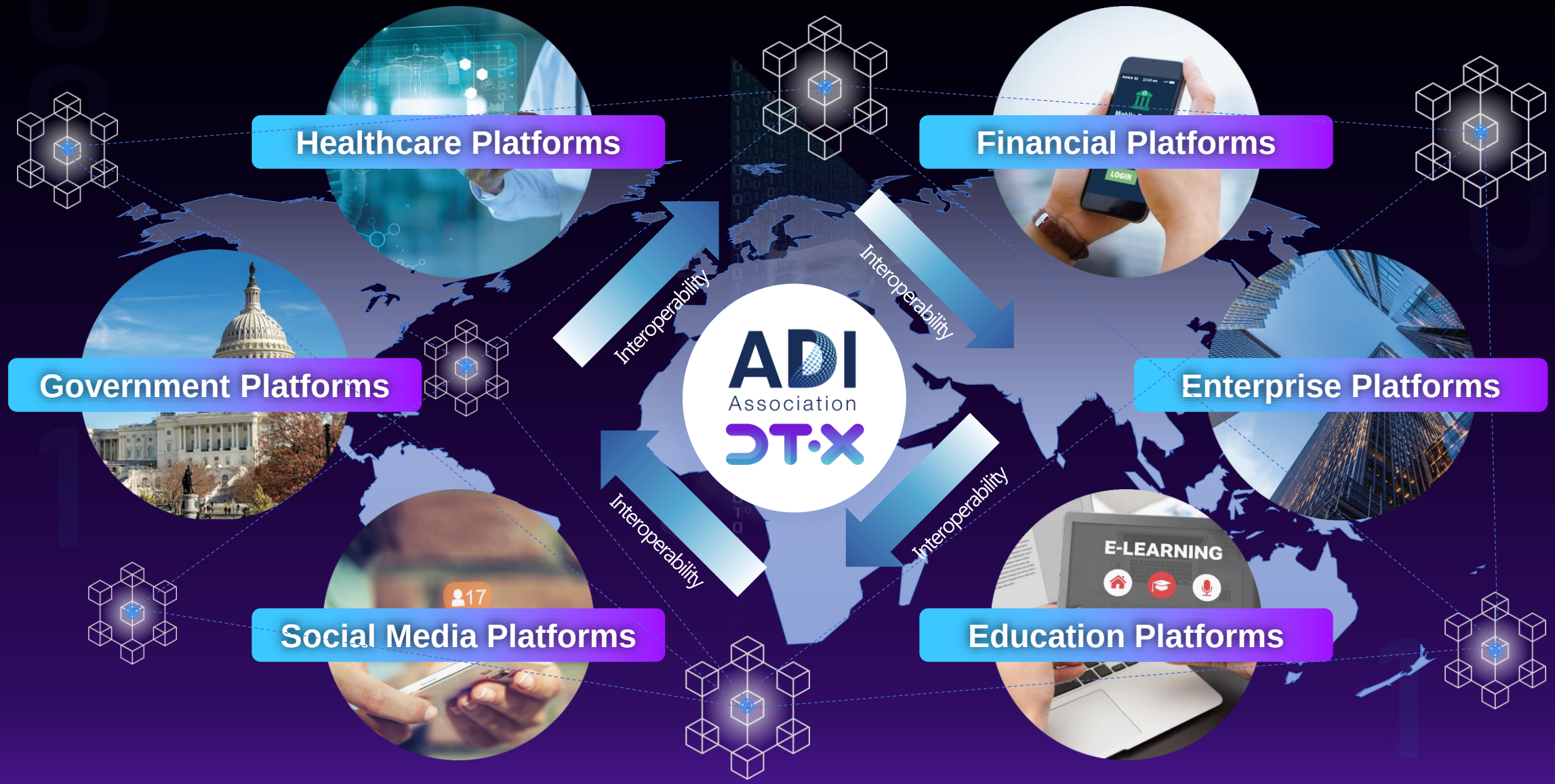
Issuers & Users Into the Value Chain

We Include All People in Digital Identity

ADIA Ecosystem



Global interoperability of ADIA interchanges



Call to Action

- Specification 2.0 work just started
- Please join the ADI Association as member
- Help Advance and Contribute to the Specification
- Extend your FIDO Implementation to add Identity to bring Accountability framework to the digital networks
- Implement ADI Framework
- Participate in Directory Service hosting

시큐업 세미나 2022

디지털 인증의 현재와 미래

모바일 신분증 신원증명

한국조폐공사 **양희선 팀장**

2022.10.04

목차

1. 한국조폐공사 소개
2. 모바일 운전면허증
3. 모바일 신분증의 미래

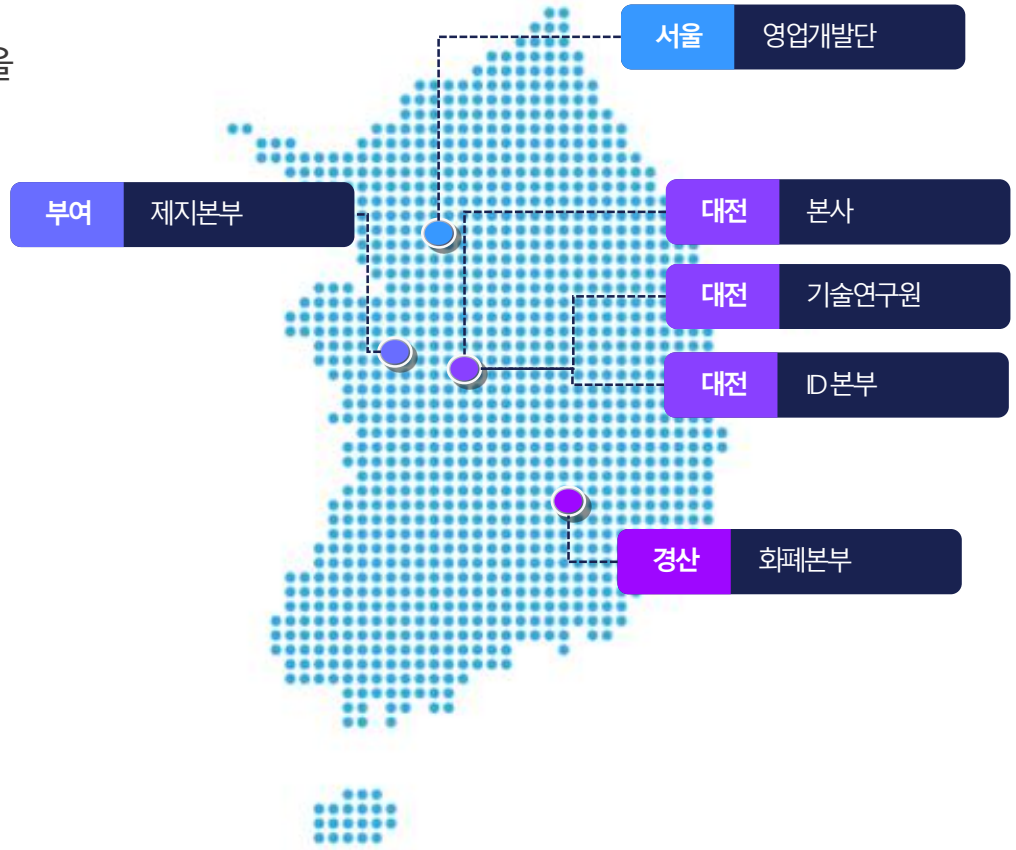
01 한국조폐공사 소개

한국조폐공사 소개

- 한국조폐공사는 1951년에 설립된 기획재정부 산하 공공기관
- 국가에서 사용하는 은행권, 주화, 각종 유가증권과 국가신분증(주민등록증, 여권, 공무원증 등)을 전담 공급하는 공기업

※설립근거: 한국조폐공사법(법률 제17156호, 2020.3.31. 일부개정

- 설립연도 | 1951년
- CEO | 반 장 식
- 직원 수 | 1,517여 명 임직원
- 매출 | 5,506억원(2021년)
- 제품 수 | 660여 가지 제품



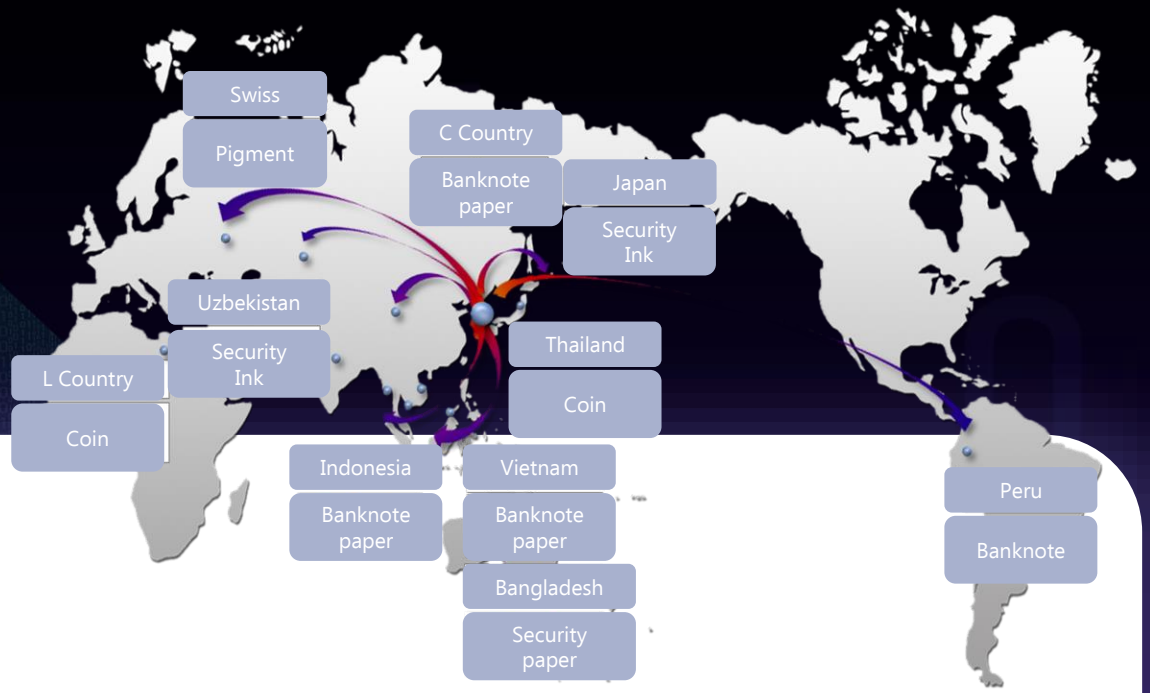
GKD GLOBAL KOMSCO DAEWOO 해외 자회사(우즈베키스탄)

한국조폐공사 사업

❖ **사업분야**

- 인쇄제품, 압인제품, 보안ID 제품, 브랜드보호 제품, 블록체인기반 모바일 상품권

❖ **해외사업 누적성과 :** 해외 47개국(7억 4670만 불)



■ **인쇄 제품 :** 은행권, 수표. 우표 및 채권류, 상품권, 특수보안용지

■ **압인 제품 :** 주화, 기념주화, 기념메달, 훈장, 골드바 등

■ **보안ID 제품 :** 주민등록증, 여권, 보안모듈 등

■ **브랜드보호 제품 :** 위·변조방지 보안 라벨, 특수물질 등

■ **블록체인 기반 모바일상품권 등**

국가 신분증 제조발급 전담기관 및 모바일 신분증 전문기관

- **국가신분증 제조/발급 전담기관 :** 주민등록증, 전자여권, 외국인등록증, 전자공무원증 등 공급
- **모바일 신분증 및 전자서명 전문기관 :** 모바일 공무원증, 운전면허증, 간편인증 시스템 구축 및 운영

KOMSCO
Korea Minting, Security Printing & ID Card Operating Corp.
한국조폐공사

- 법적 근거에 따라 각종 국가신분증 제조 및 발급 수행
  - ✓ 한국조폐공사법 "제11조5항"
- 국가 유일의 보안인쇄 전문기관
- 국가신분증(주민등록증, 전자여권, 공무원증 등) 제조 및 발급 인프라 보유
- 국가 모바일 신분증 및 전자서명 전문기관 지정

1951 KOMSCO 설립

국가신분증 제조•발급

2022	모바일 국가유공자증 구축
2021	모바일 신분증 및 전자서명 전문기관 지정 모바일 운전면허증 구축 및 운영
2020	모바일 공무원증 구축 및 운영
2013	전자공무원증 제조발급 전담기관
2008	전자여권 제조발급 전담기관
2002	외국인등록증 제조발급
1999	주민등록증 제조발급 전담기관

02 모바일 운전면허증

대한민국 3대 신분증

주관기관

근거법령

형태

주민등록증

행정안전부

주민등록법

플라스틱 카드
(위변조 방지기술 적용)

전자여권

외교부

여권법

IC 칩이 탑재된
전자여권

운전면허증

경찰청

도로교통법

플라스틱 카드
(위변조 방지기술 적용)

정부기관이 근거 법령에 의해 발급함으로써

국가가 개인의 신분을 공식 증명하는 문서

모바일 운전면허증

모바일 운전면허증 앱

+

전자여권과 동일한 IC칩이 탑재된

IC 운전면허증

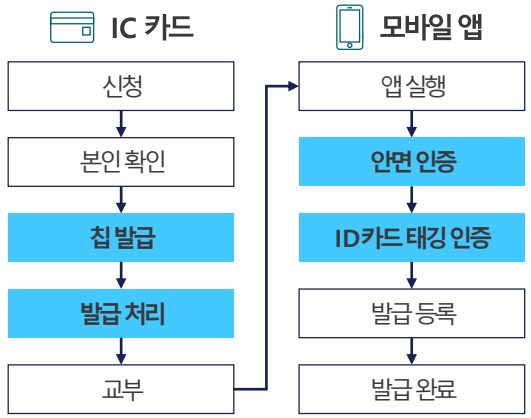
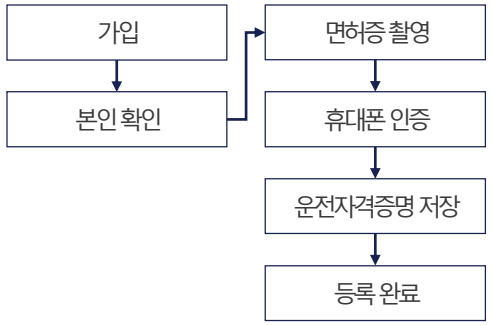
모바일 운전면허증

- 도로교통법에 따라 지방경찰청장이 개인 스마트폰에 암호화하여 안전하게 발급/저장하는 운전면허증

- '22.1.27(목)부터 도로교통법 시행규칙 개정으로 모바일 운전면허증이 운전면허증의 한 종류로 규정됨에 따라 모바일 운전면허증에 **현행 실물 운전면허증**과 **동일한 법적 효력**이 부여됨

모바일 운전면허증 목표

❖ 민간의 유사서비스와는 근본적으로 다른 全국민 대상 국가신분증 구축

	국가 모바일 운전면허증	민간 본인확인 서비스
절차	 엄격한 신분증 발급절차	 既 등록된 신분증 단순 조회서비스
기술	탈중앙화 신원 인증 (DID)	중앙집중형 신원 인증 (CID)
증명 주체	사용자 중심 (자기 주권 신원 증명)	서비스 제공자 중심
용도	범용적 활용 (신분증과 동일 효력)	제한적 활용 (편의점 성인인증 등)

특징

신분증의 공신력을 보장하는
발급절차 설계 중요

全 국민 대상의
국가적 디지털 전환사업

DID 기술 기반
자기주권 신원증명 본격 적용

*DID : Decentralized Identifier CID : Centralized Identifier

모바일 운전면허증 사업(목적)

휴대폰 하나로 어디서든 내가 원하는 정보로 신원을 인증

발급/운영기관

발급 KoROAD 도로교통공단

운영 KOMSCO 한국조폐공사

공신력 있는
신분증 발급/운영기관

이용자

자기 주권 신원 (SSI)

온-오프라인 통합인증

서비스 제공기관

공공	공공웹 인증	증명서 발급	…
금융	은행 계좌개설	증명서 발급	…
민간	렌터카 이용	편의점 성인인증	…

신원검증

*SSI : Self-Sovereign Identity

분산신원증명(DID) 블록체인 플랫폼

국가 신분증으로서 공신력 보장

안전하고 신뢰할 수 있는 국가 공통 플랫폼 구축

유용하고 쓰임새 많은 국민 체감형 서비스 확대

모바일 운전면허증 DID, DID 문서, VC, VP

❖ DID(Decentalized Identity, 분산ID)

- 탈중앙화된 신원 정보
- 자기 주권 신원 (SSI, Self-Sovereign Identity) - 이용자가 스스로 개인의 정보를 통제

❖ DID 문서

- DID 메타 데이터 및 인증수단, 공개키가 포함된 구조화된 문서

❖ VC(Verifiable Credential)

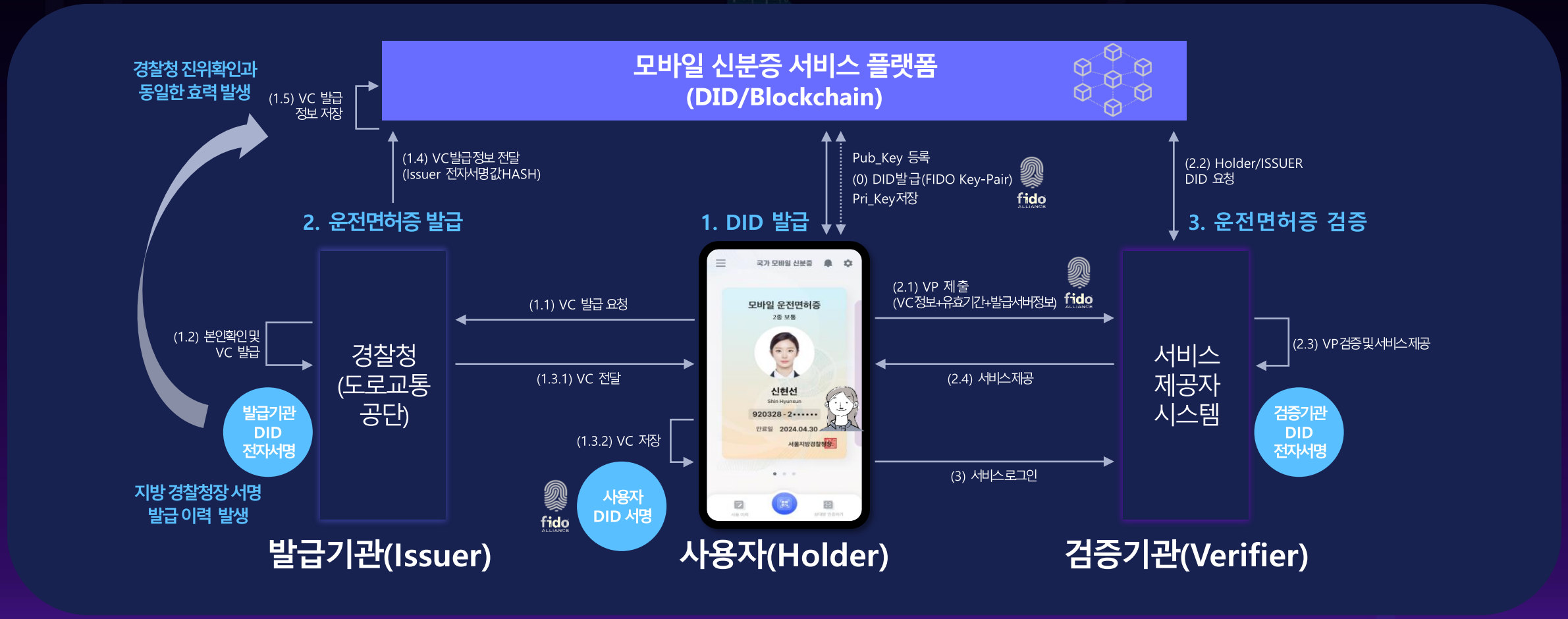
- 검증 가능한 자격 증명
- ID 데이터 또는 클레임들과 발급자를 암호학적으로 검증할 수 있는 메타 데이터의 집합

❖ VP(Verifiable Presentation)

- 검증 가능한 제출정보
- 신분 또는 자격을 설명하는 정보에 대한 일부분의 조합

모바일 운전면허증 블록체인 플랫폼

❖ 모바일 신분증 서비스는 FIDO와 DID 기술을 사용하여, 증명 가능한 기관으로부터 발급받은 신원정보를
스마트폰의 안전 영역에 보관하고, 정보가 필요한 기관에게 이용자가 직접 정보를 제출하여 검증 받는 블록체인 기반 분산 ID 플랫폼



모바일 운전면허증 블록체인 플랫폼 신뢰성

❖ **한국정보통신기술협회**

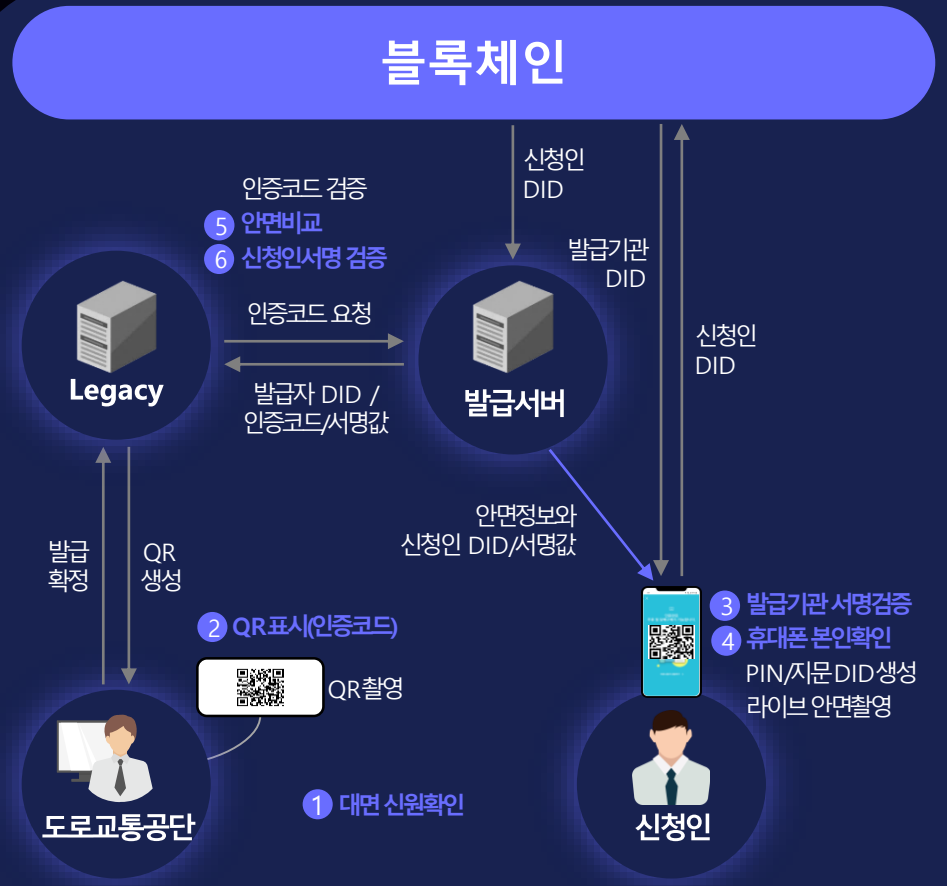
- 블록체인 플랫폼·신분증앱 등에 대한 신뢰성(보안성·성능) 컨설팅 및 시험을 수행

검증속성	검증항목	* 내용
효율성 (성능)	블록 확정 성능	데이터 입력 시 트랜잭션 및 블록의 완결성 보장을 전재한 초당 트랜잭션, 또는 업무처리 건수
	블록 참조 성능	데이터 조회 시 초당 트랜잭션, 또는 업무처리 건수
	용량 확장 성능	최대 트랜잭션, 블록크기 도달 시의 처리성능
	노드 확장 성능	가정된 최대 노드 참여 시의 처리성능
호환성	타 시스템 연동	API 서버, 외부 DB 등 타 시스템과의 상호연동 기능
가용성	노드장애 대응	특정 노드 장애 시 전체 시스템의 블록 동기화 기능
	노드구성 적합성	사업계획 및 합의기술에 적합한 방식으로 노드구성
보안성	기밀성	블록 내에 민감한 데이터 보호를 위한 암호화 기능
	무결성	블록 내에 저장된 데이터의 위변조 방지를 위한 기능
	권한제어	사용자 접근제어, 트랜잭션 생성 권한제어 기능
	취약성 대응	블록체인 플랫폼 및 서비스의 알려진 취약성에 대한 보안대책 ✓ **스마트 컨트랙트 대한 소소코드 보안 취약점 별도 실시**

모바일 운전면허증 발급 보안

❖ 모바일 신분증 발급 3원칙

- 반드시 정당한 신청자에게만 발급
- 반드시 대면 확인한 신청자 본인의 휴대폰에만 발급
- 발급시스템의 신뢰성을 증명



신분증 발급 3원칙에 기반한
6단계 인증 적용

1. 최초발급 시 **대면 신원확인**
2. 신청인 전용 **QR생성/검증**
3. 발급기관 **서명값 검증**
4. 휴대폰 **본인확인**
5. 면허증사진 vs **촬영안면비교**
6. 신청인 **서명값 검증**

- 강력한 6단계 인증절차를 통해 신청인과 모바일 신분증 간 Strong Binding 보장
- 철저한 신원검증 절차 적용으로 국가 신분증으로 공신력 및 신뢰성 보장

모바일 운전면허증 자기주권 신원증명

❖ 상황에 맞게 꼭 필요한 정보만으로 신원 증명의 신뢰성 확보

- 영지식부터 실명증표까지 개인이 목적에 따라 자유롭게 사용
- 자기 주권 신원에 따라 제출 용도, 사용 환경 별 최소한의 범위로 정보를 제공

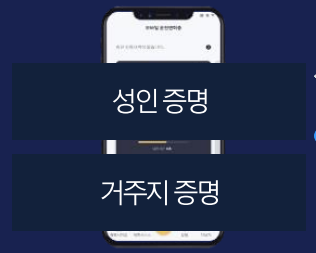
다양한 사용환경, 제출 용도에 따른 온/오프라인 통합 신원 자격증명

- 오프라인 — 편의점에서 주류 구매
- 온라인 — 휴대폰 설문조사
- 온라인 — 정부24 로그인
- 오프라인 — 경찰관에게 면허증 제시
- 온라인 — 은행 대면/비대면 계좌개설

인터넷

다양한 통신수단

영지식 기반 개인정보 노출 無



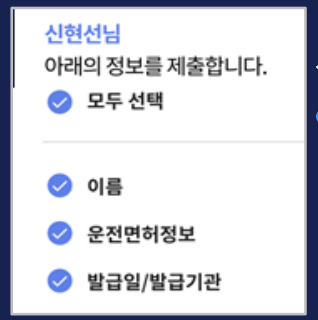
영지식 증명

성인여부 요청

성년 증명하기

증명확인 요청이 정상적으로 이루어졌습니다.

DID 기반 선택적 제공으로 도용 방지



사용자서명 VP 제출

신분증 제시 요청 / 검증

사전 허가된 정책 기반 정보 제공

서비스 프로파일

사용자서명 VP 제출

신분증 VP 요청 / 검증

읽기 노드

제공범위, 용도, 기한 내에서만 검증 및 사용

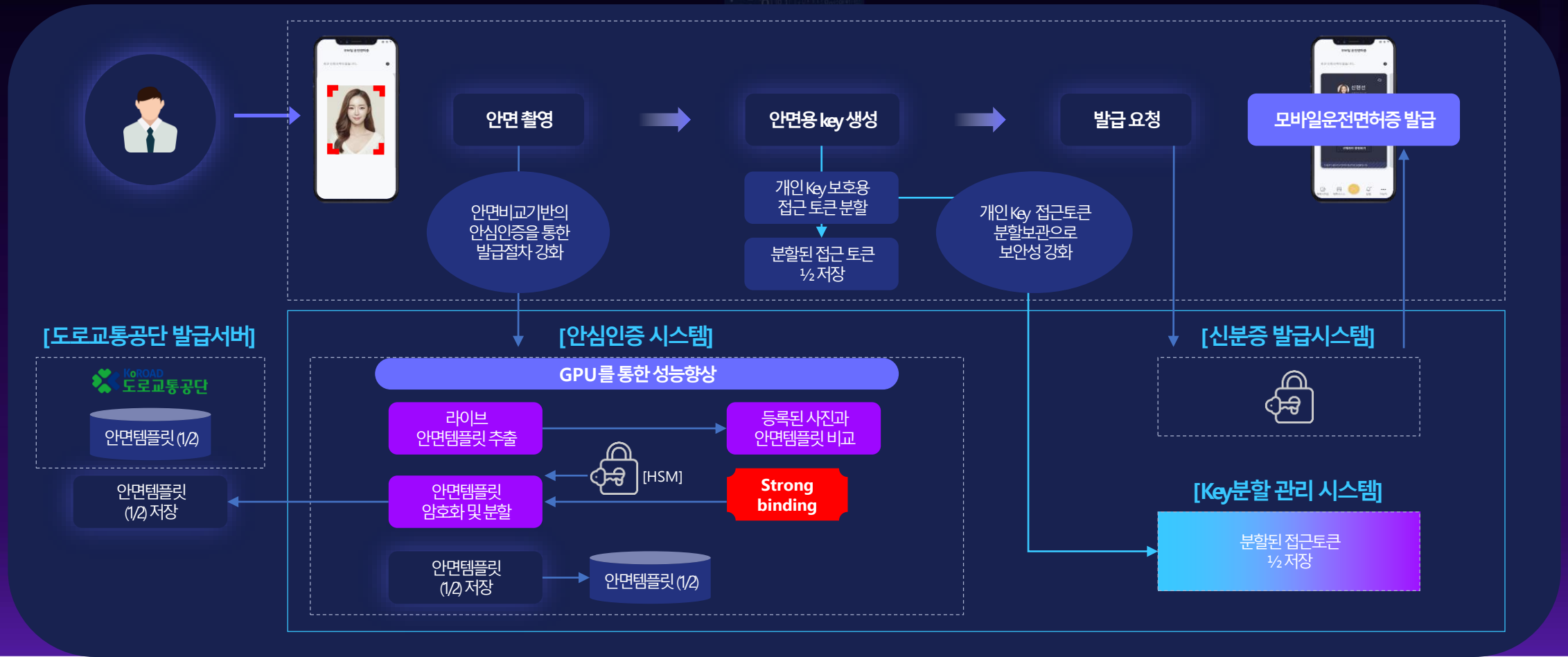
모바일 운전면허증(안심인증)

❖ 안심인증 사용 이유

- 정당한 소유자가 발급•제출했는지를 사전에 등록된증명사진과 비교•검증하여 사용자 인증을 강화

❖ 안심인증 성능

- FAR(False Accept Rate) 1:100,000 이하
- FRR(False Reject Rate) 5% 미만
- SAR(Spoof Accept Rate) 3% 미만



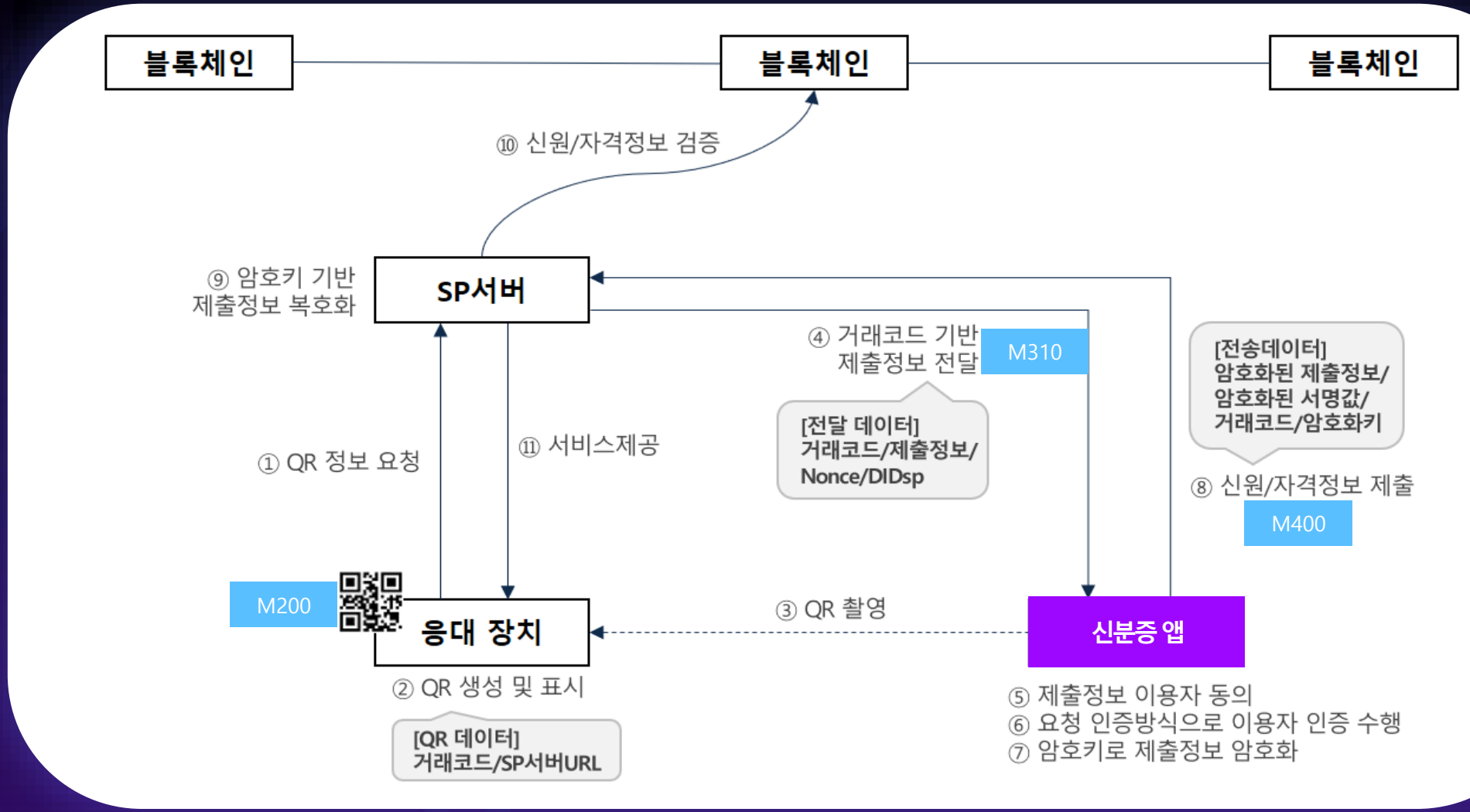
모바일 운전면허증 : 프라이버시 보호

❖ **영지식증명(ZKP)**
- 상대에게 무언가를 증명하는 데 있어 제3자나 상대방이 내 비밀정보와 관련한 어떠한 지식(정보)도 얻지 못하게 하는 방법

❖ **신원증명 내역에 대해 제3자가 알 수 없도록 설계**
- 신원증명 내역에 대해, 영지식용 VC는 Type3 기반으로써 DID와의 연결성을 제거하여 제출한 소유자와의 특정가능성을 완전배제
- 영지식증명(ZKP)을 통한 특정 가능성 제거

구분	항목	조건 여부	비고
단일 성인	성인여부	나이 조건 있음	조건 이상 시 Y, 아니면 N
단일 기타	주소	조건 없음	시, 군, 구 까지 제공
	성별	조건 없음	남, 여
	면허종별	조건 없음	1종, 2종 등
복합	성인여부+주소+성별+면허종별	조건 있거나 없음	항목별 조합 가능

모바일 운전면허증 인증방식



QR-MPM	Merchant Presented Mode
QR-CPM	Customer Presented Mode

모바일 운전면허증 전국 발급

❖ **모바일 운전면허증 '22.7.28.(목)부터 전국 발급**

- 공공·금융기관, 편의점, 렌터카업체, 병원, 선거, 시험(국가기술자격, 토익), 공항 탑승 수속 등 다양한 분야에서 사용 중
- (전국 발급)27개 운전면허시험장 및 258개 경찰서

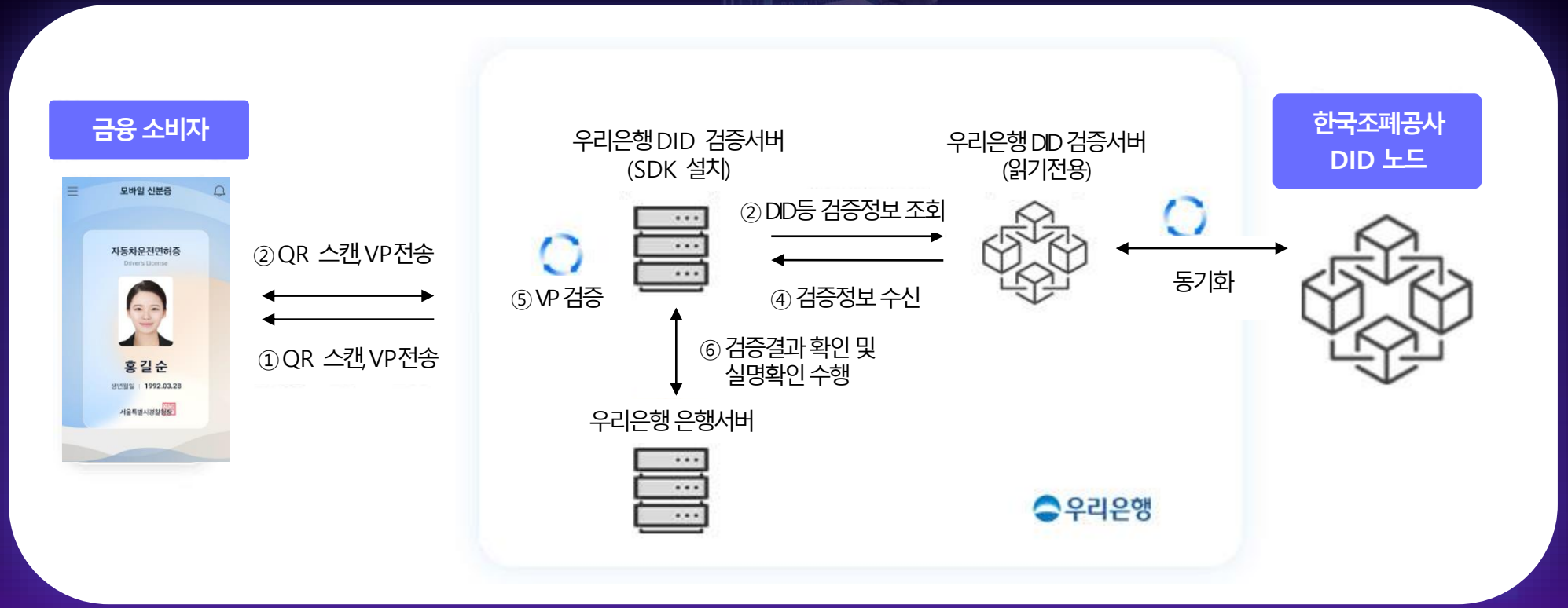
모바일 운전면허증 사용 예

❖ **금융거래(대면/비대면)**

- 13개 은행의 영업점 창구와 4개 은행의 스마트폰 앱을 통해서 금융거래
- '22.하반기에는 대부분의 은행에서도 금융거래 가능

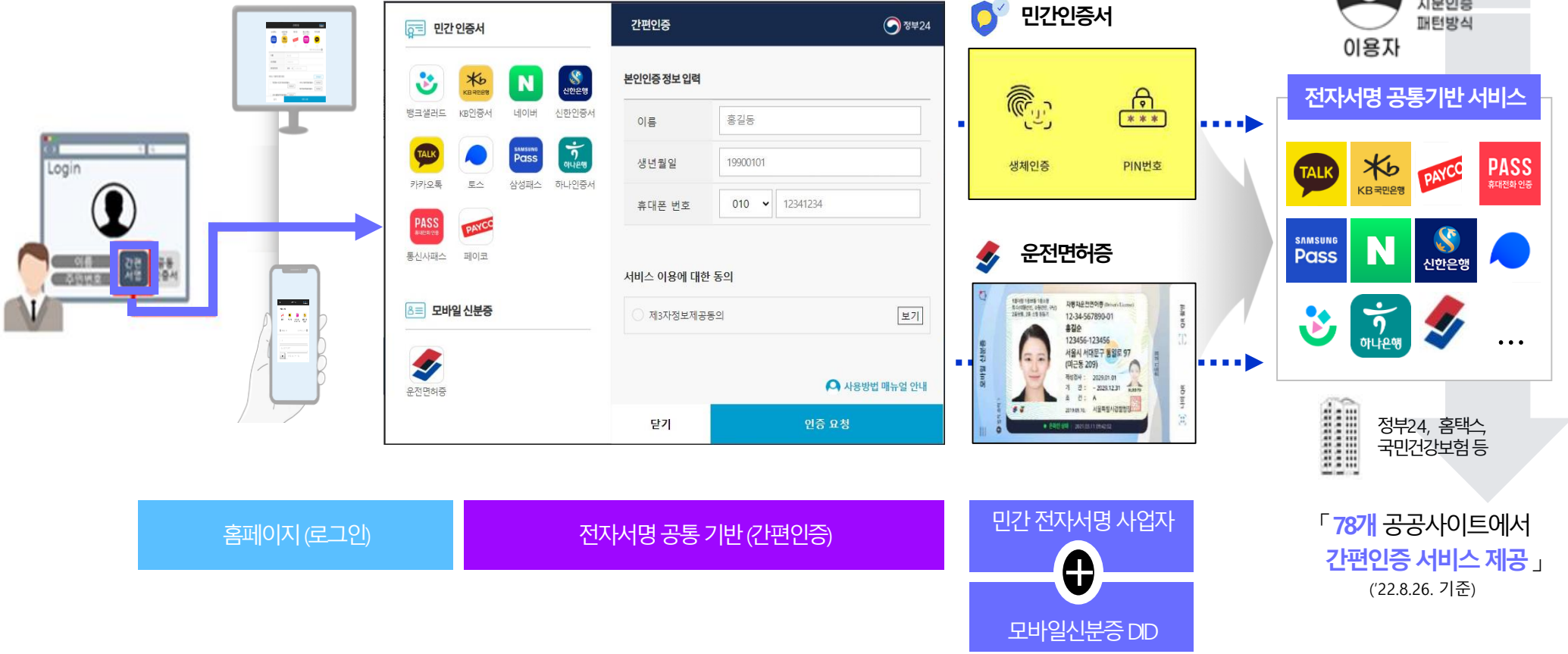
❖ **우리은행 : 모바일 운전면허증으로 대면 실명확인**

- 모바일 신분증 시스템과 연계한 은행 단말기에서 QR코드를 생성하고, 이를 사용자가 스캔하여 인증하면 사용자의 실명확인



모바일 운전면허증 사용 예

❖ 공공 포탈 접속 시 온라인 본인인증 : 정부24 등



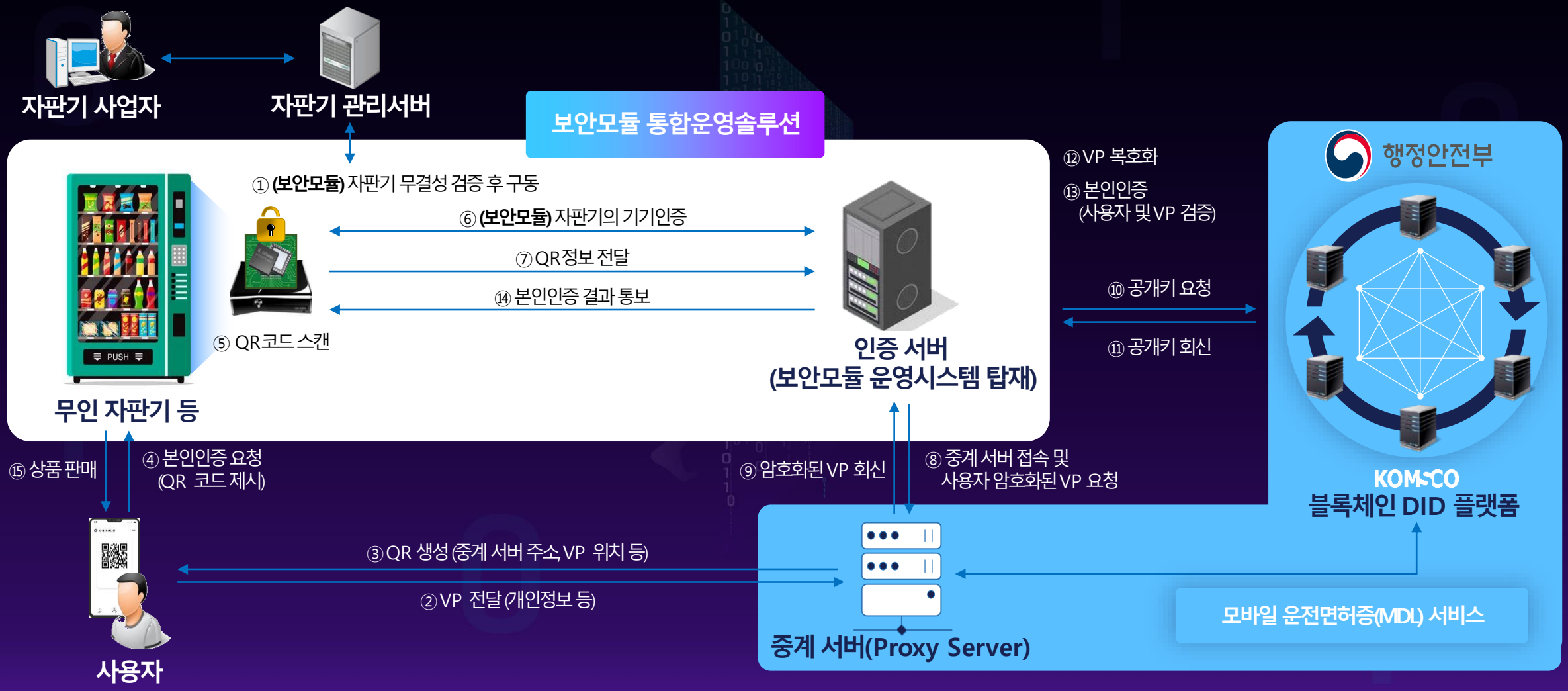
모바일 운전면허증 사용 예

❖ 성인인증

- **CU와 GS25 :** 술, 담배 등 19세 이상 구매 대상 상품 구매
- **페이즈커뮤 등 :** 무인 스낵주류 판매기 성인인증
- **휴대폰 가입 :** 통신사

모바일 운전면허증 사용 예

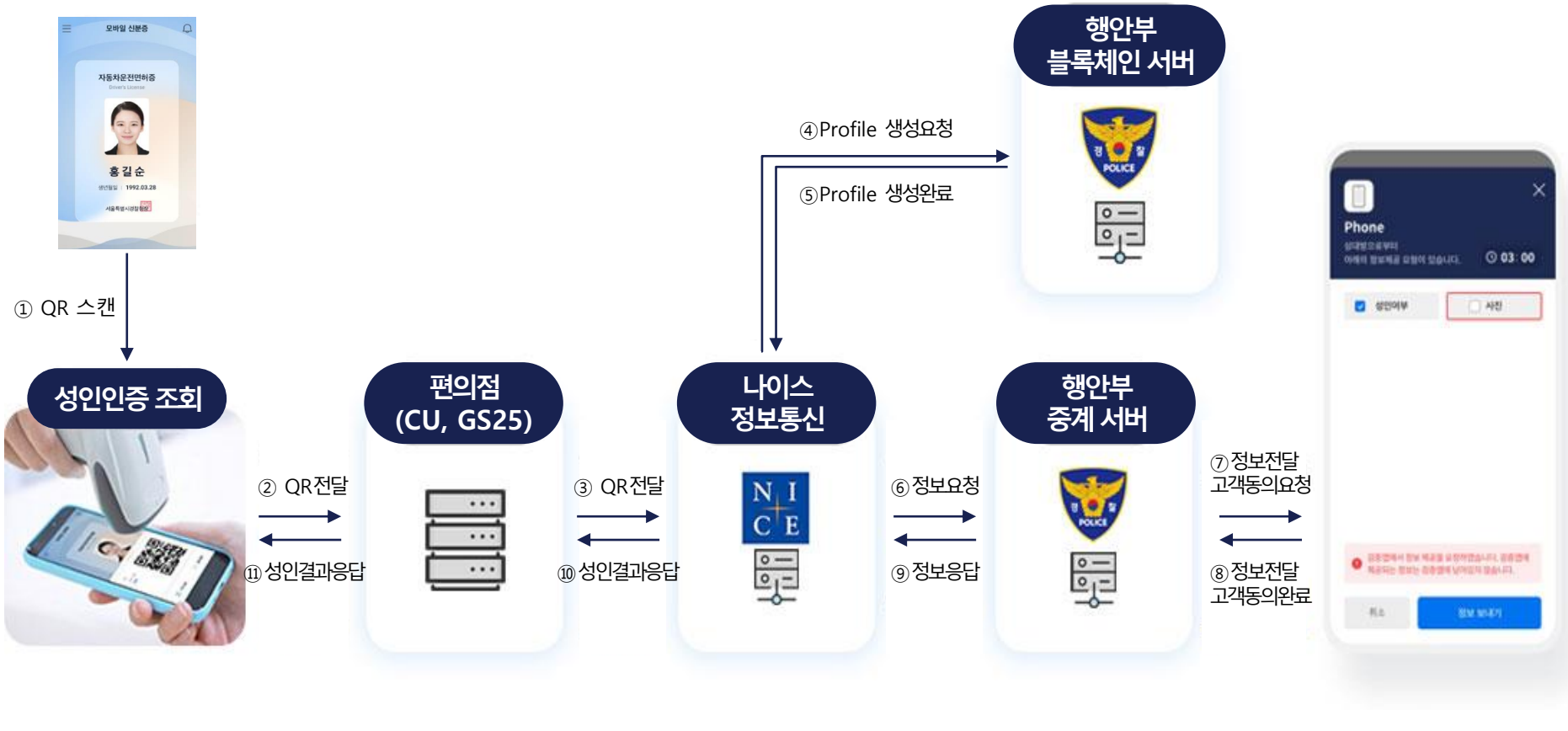
❖ 성인인증 세부 내역 시스템



모바일 운전면허증 사용 예

❖ **성인인증 : 나이스 정보통신**

- 모바일 신분증 앱을 통한 QR코드를 표시하여 응대장치를 통한 QR 스캔 및 중계서버를 통한 신원/자격제출 정보에 대한 검증 요청

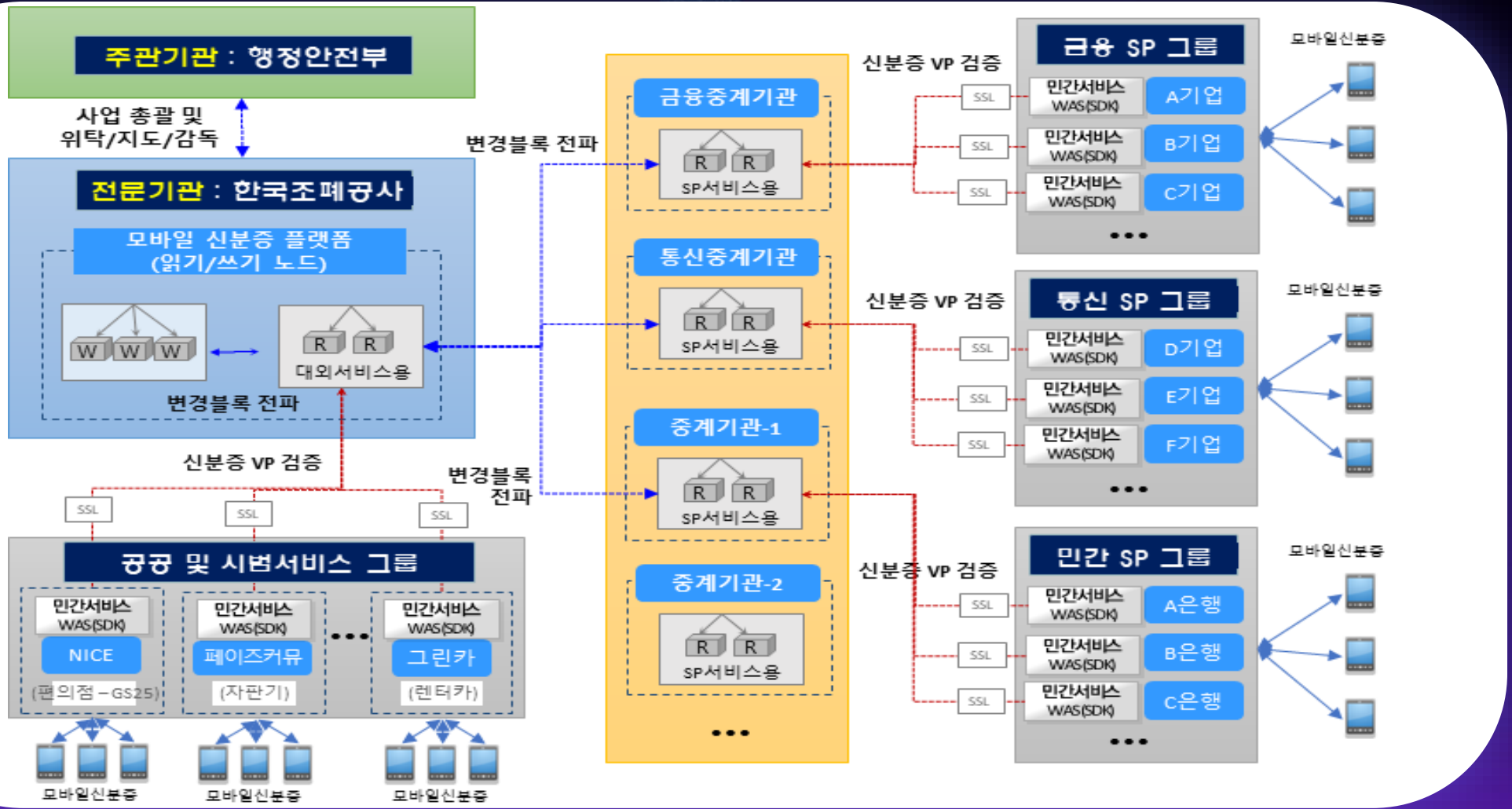


모바일 운전면허증 사용 예

- **숙박시설 무인 체크인 :** 야놀자 등
- **실명확인 서비스 :** 하나증권 등
- **송금 서비스 :** 네이버 페이 등

모바일 운전면허증 리드노드 운영기관 선정

- ❖ 국민이 일상생활의 다양한 분야에서 모바일 신분증을 불편없이 이용할 수 있도록 모바일 신분증 이용 활성화가 필요
- ❖ 모바일 신분증 활성화를 위해 서비스 제공처(SP) 확산 필요
  - 리드노드(블록체인 노드 중 읽기 기능만 가능한) 운영자 선정을 통한 자생적 생태계 조성을 통해 운영 서비스 활성화 추진



모바일 신분증 클라우드 인프라

- ❖ 모바일 운전면허증의 클라우드 서비스 부분은 공사에서 구축운영
- ❖ 최고의 보안시설 구축

03 모바일 신분증의 미래

모바일 신분증의 미래

“국민의 일상을 새롭게 바꾸는 디지털 신분증”

신뢰성

안심하고 쓸 수 있는 든든한 신분증

신분증 특화 안심기술
디지털 신분증 생애주기 관리

활용성

생활이 즐거워지는 편리한 신분증

누구에게나 편리한 UX 온/오프라인
신원 인증 환경의 일원화

DID / 블록체인 기반
국가 공통 플랫폼 구축

모바일 신분증의 미래

❖ 대국민 블록체인 DID 국가 디지털 신분증 플랫폼 구축

기술검증 (2020)

모바일 공무원증

행정안전부, 인사처

전국민 모바일 신분증 시대를 위한 첫 관문

DID/블록체인 기반
모바일 신분증 플랫폼

(2021)

국가 신분증 플랫폼 구축 및 운영

모바일 운전면허증
(경찰청, 도로교통공단)

(2022~)

국가신분증 운영 및 확대

- 국가유공자증(국가보훈처)
- 주민등록증, 장애인 신분증
- 청소년증, 외국인등록증
- **공공민간 융합 서비스**
- **각종 민원 서비스 연계 검토 및 설계**

DID/블록체인 기반
국가신분증 공통플랫폼

"대국민 블록체인 DID 국가 디지털 신분증 플랫폼"

Trustful Identity

국가가 발급 공신력 있는 신분증

Convenient Mobility

온/오프라인 통합형 신원인증 체계

Self-Sovereign Model

신원주체가 직접 자신 정보 보유,
필요한 곳에 필요한 정보만 제공

시큐업 세미나 2022

디지털 인증의 현재와 미래

인증 서비스의 새로운 기준, 옴니원 통합인증 서비스

라온화이트햇 **김태진 전무**

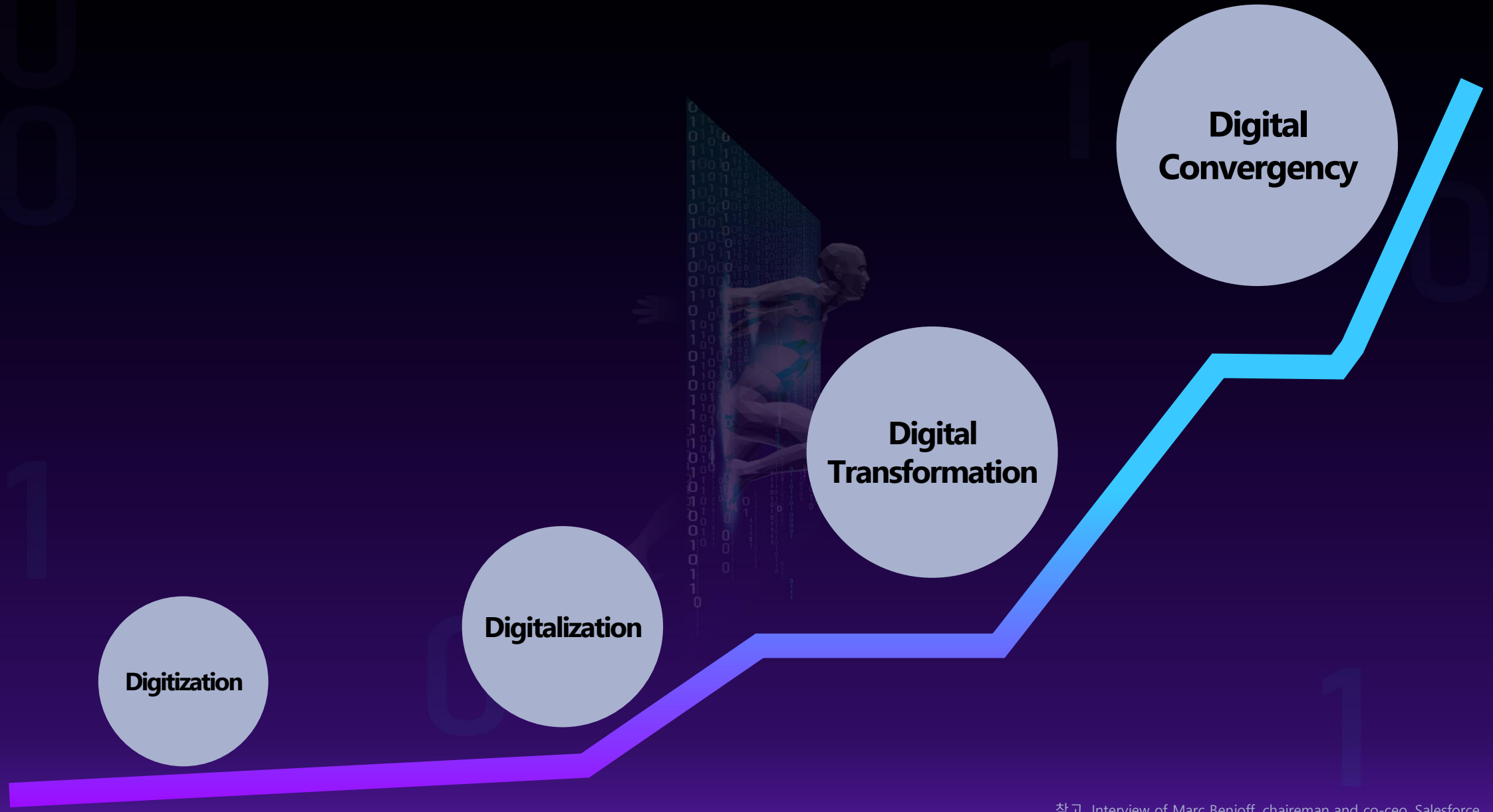
2022.10.04

목차

1. 디지털 전환 가속화
2. 통합인증 서비스의 시대
3. 서비스 확장 및 글로벌화

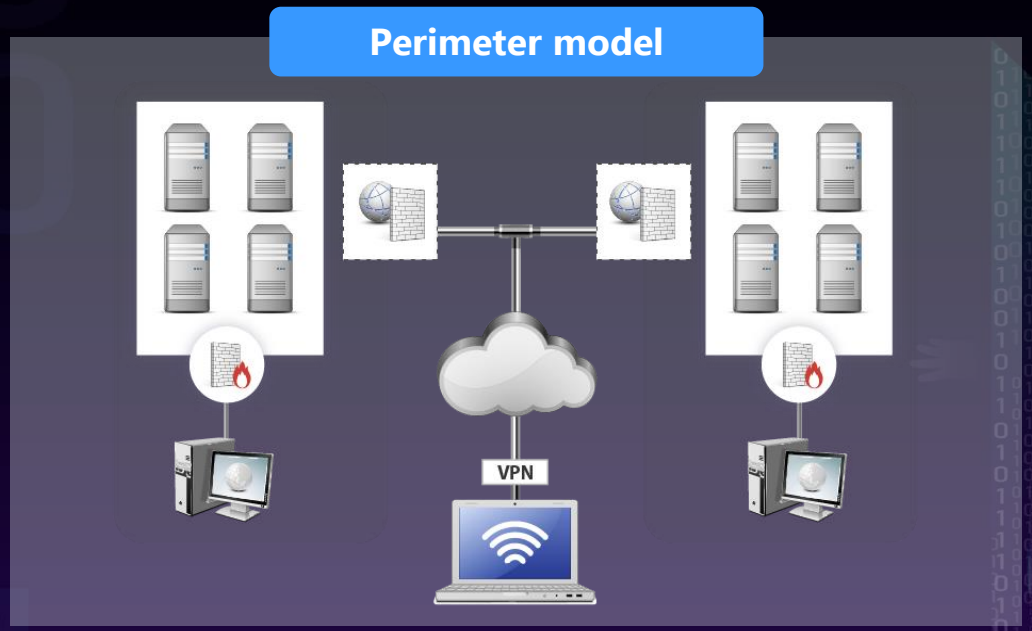
01 디지털 전환 가속화

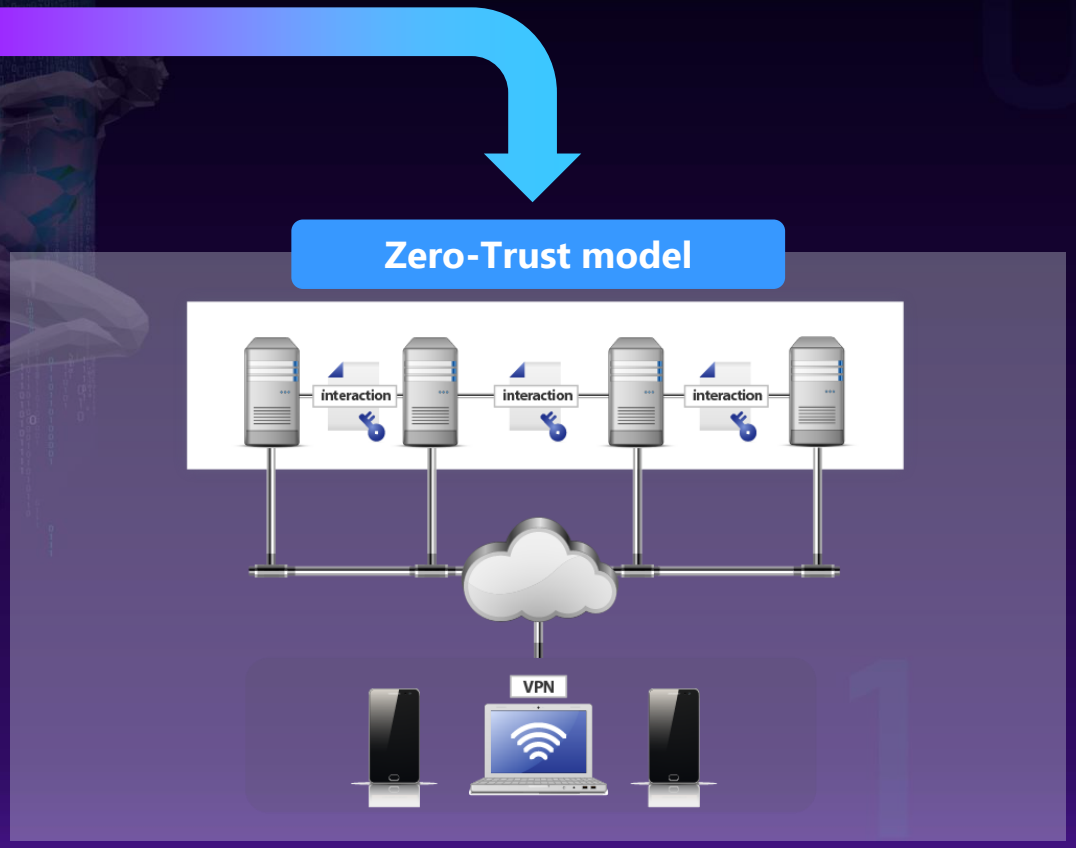
1. 디지털 전환 가속화



참고. Interview of Marc Benioff, chaireman and co-ceo, Salesforce

1. 디지털 전환 가속화


Perimeter model
VPN


Zero-Trust model
interaction
interaction
interaction
VPN

1. 디지털 전환 가속화

*이미지. 6 Ways Colleges And Universities Are Responding To Coronavirus
출처. https://www.npr.org/2020/03/06/812462913/6-ways-universities-are-responding-to-coronavirus

COVID-19 팬데믹

비대면 환경으로의 전환 가속화

Zero-Trust Security 기반의 DX 변화

사용자의 온라인 아이덴티티 식별 중요

02 통합인증 서비스의 시대

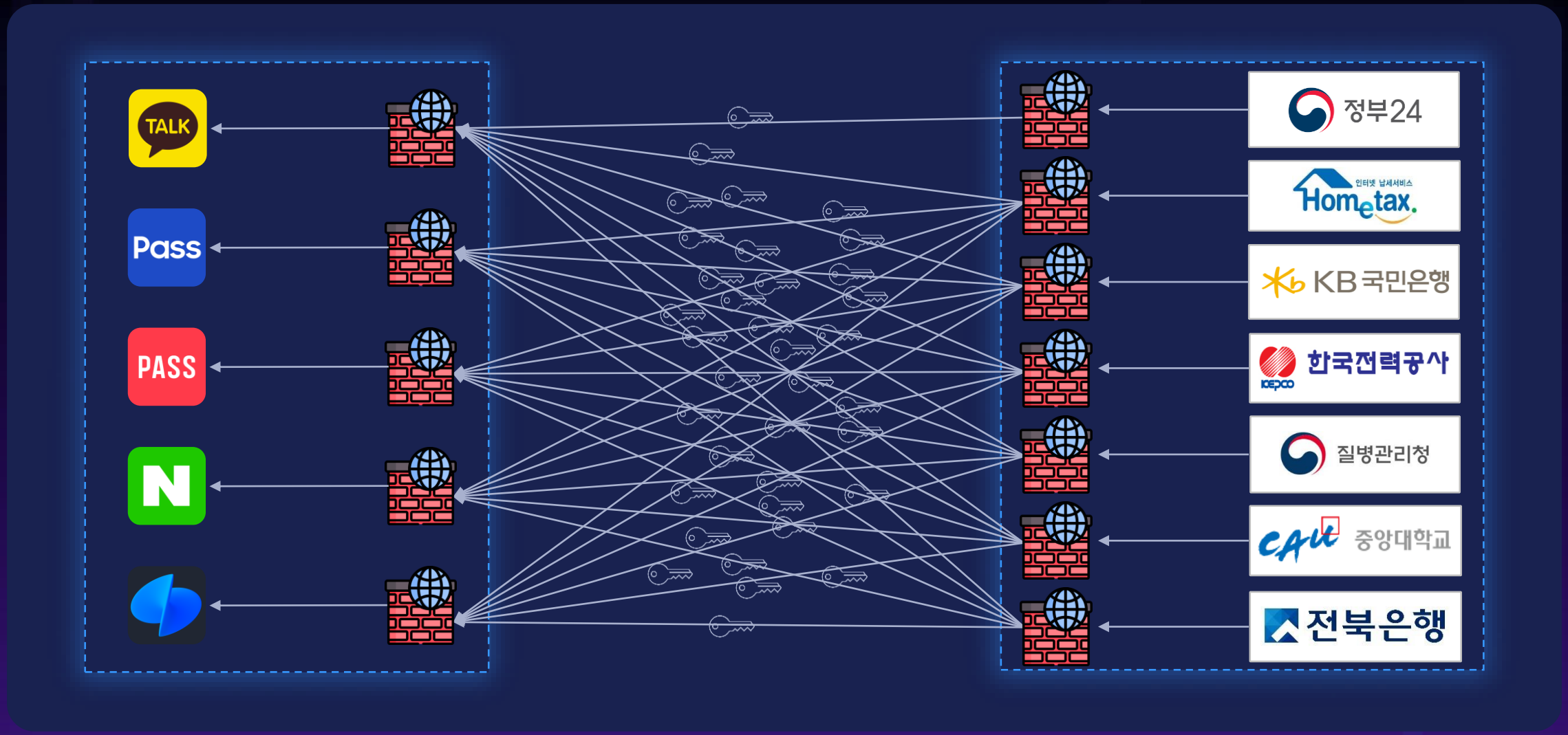
전자서명법 개정에 따른 **전자서명수단 간의 경쟁 활성화**

▷ 2020년 6월 9일부터 전자서명법 개정

- 전자서명인증 업무 운영기준 준수 사실 평가 및 인정제 도입

전자서명 인증업무 평가·인정 제도 도입으로 블록체인, 생체인증 등
신기술 기반의 다양한 전자서명 개발, 이용 활성

2. 통합인증 서비스의 시대



2. 통합인증 서비스의 시대

수많은 디지털 증명서, 모바일 신분증, 사설 인증서를
전부 통합할 수 있는 서비스가 어디 없을까?

2. 통합인증 서비스의 시대

2. 통합인증 서비스의 시대

단 한 번의 연결	개발의 편리 / 통합 정산관리	인증 수단의 다양화
옴니원 통합인증 서비스로 **모든 모바일 신분증 디지털 증명서 사설 인증서 이용 가능**	개발의 편리함과 통합 정산 관리 등으로 **도입 비용 절감 효과 발생**	다양한 인증 서비스 제공을 통해 **고객만족도 제고 가능**

OMNIONE

통합인증 서비스

‘통합인증’의 패러다임을 선도

디지털 시대에 필수적인
복잡한 신원인증, 자격검증 절차를 편리하고 간편하게 구현

2. 통합인증 서비스의 시대

정부 24앱의 통합인증 서비스 구현 사례

정부 24 로그인

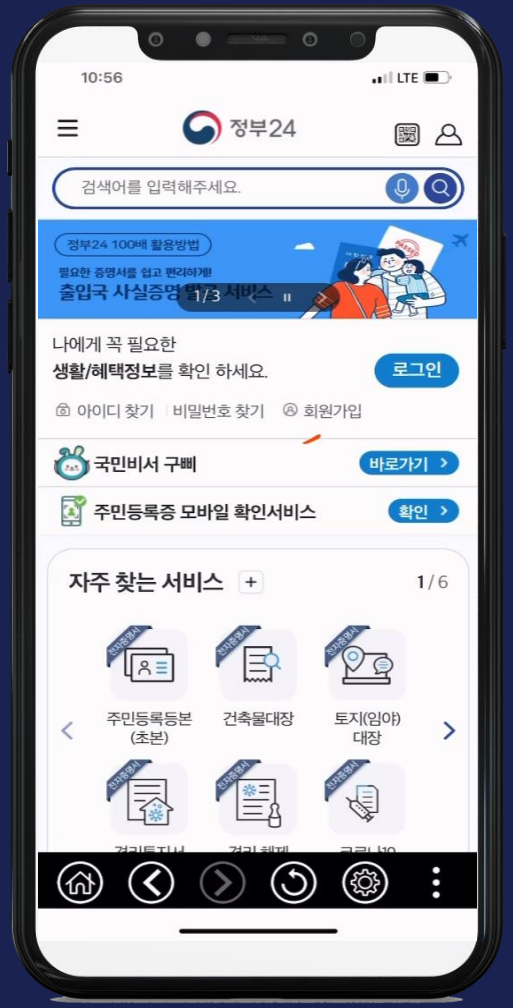
인증서 ▶ 간편인증

모바일 운전면허증 선택

모바일 신분증 앱에서
신원정보 요청 승인

생체 / 비밀번호 인증

로그인 완료



2. 통합인증 서비스의 시대

현시점(서비스 제공 중)	1단계	2단계
OMNIONE 구축형 서비스	OMNIONE 클라우드형 SaaS 서비스	OMNIONE 글로벌 통합인증 서비스
2021년 4분기 사설인증 검증 중계시스템 출시 2022년 1분기 모바일 신분증 / 디지털 증명서 중계 시스템 출시	2022년 4분기 모바일 신분증 / 디지털 증명서 / 사설인증용 클라우드 기반 옴니원 통합인증 서비스 출시	2023년 2분기 ADI 국제표준 기반 글로벌 옴니원 통합인증 서비스 출시 예정

03 서비스 확장 및 글로벌화

3. 서비스 확장 및 글로벌화

Most people are thinking

Your Identity == App(authenticaiton)

However,

Your Identity > App(authenticaiton)

And,

Your Identity > ID Card

참고. MS Build SK114 Building trust into digital experiences with DID

3. 서비스 확장 및 글로벌화

Identity is everything you do

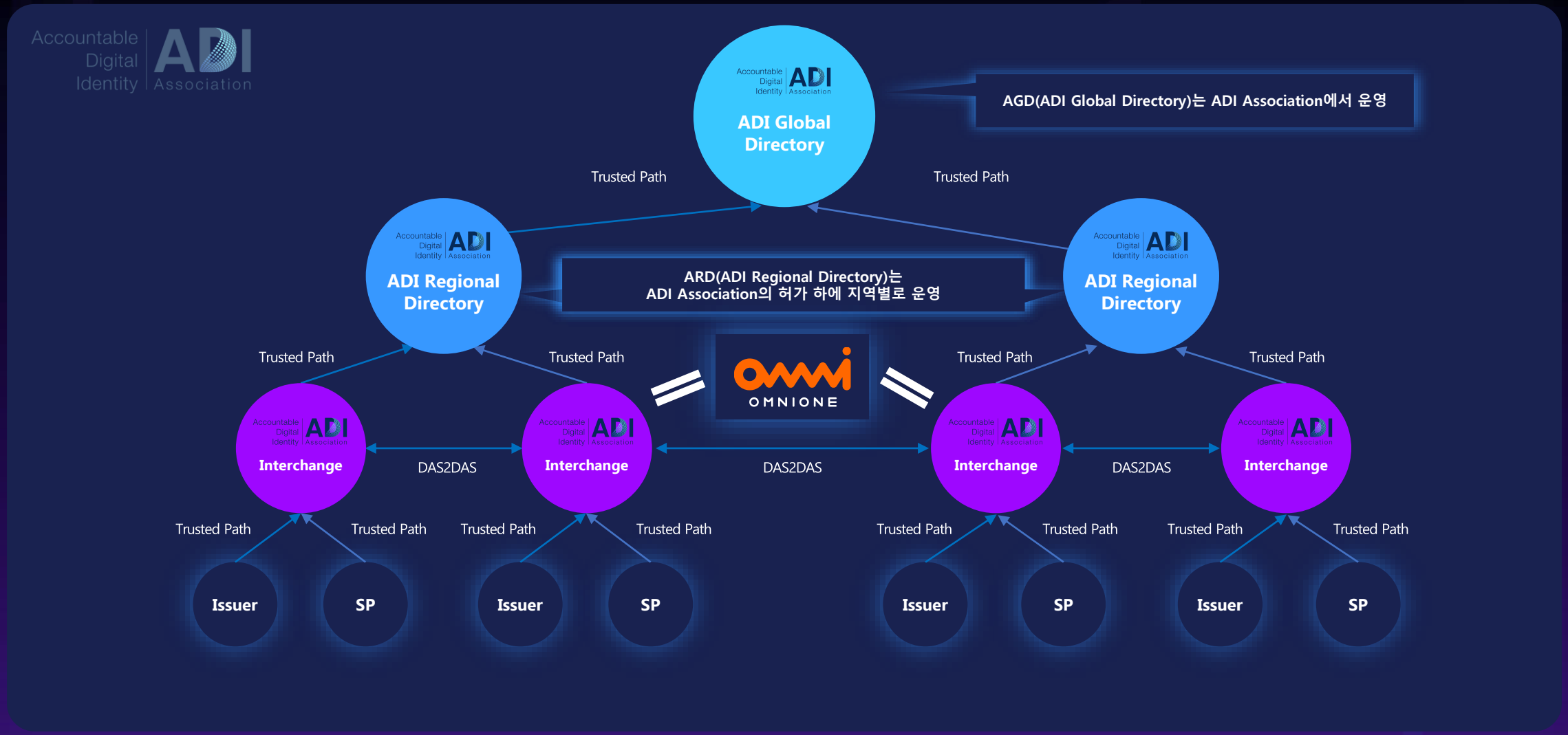
But, our identities are strewn across apps and services.

참고. MS Build SK114 Building trust into digital experiences with DID

Future requirements

- Privacy and control of my identity and data
- Trust and verify
- Collaborate with everyone
- Global Interoperability

3. 서비스 확장 및 글로벌화



기대효과

- ✓ 아이덴티티 기술 기반 데이터 교환 표준 에코시스템 조성
- ✓ 엔티티 간 신뢰성 보증 및 프라이버시 보호 강화
- ✓ 신규 비즈니스 창출 및 확대를 위한 기술 개방
- ✓ 이기종 에코시스템 간 글로벌 신뢰 프레임워크 구축

한국디지털인증협회

Accountable Digital Identity ADI Association

시큐업 세미나 2022

디지털 인증의 현재와 미래

국민의 다양한 전자서명수단 선택권 제공 방향

다양한 전자서명수단의 차별 없는 경쟁환경 조성

KISA **박정효 책임연구원**

2022.10.04

국민의 다양한 전자서명수단 선택권 제공 방향

전자서명법 제 · 개정 추진경과

공인인증서는 전자서명 제도 초기의 빠른 인프라 구축에 기여

공인전자서명의 법적 우위에 따른 시장 독점 발생

전자서명 신기술 발전 저해 및 서비스 혁신 저해

Active-X 기반 서비스로 인한 운영체제/브라우저의 호환성 문제
Window와 IE에 종속적인 서비스

저장방식과 배포방식으로 인한 보안상의 문제점
보안토큰이 아닌 일반 영역 내(HDD 등) 저장

추진경과

- 1999. 02 - 전자서명법 제정 / 1999. 07 - 전자서명법 시행
- 2015. 03 - 금융, 전자금융업자의 인증방법을 완전 자율화
  인터넷뱅킹 등 전자금융거래의 공인인증서 의무사용 폐지
- 2018. 03 - 전자서명법 전부개정안 입법예고(과학기술정보통신부)
- 2020. 12 - 전자서명법 전부개정안 시행

전자서명법 전부개정안 주요 내용

전자서명수단 간 경쟁 활성화	정부의 공인전자서명의 법적 우위를 폐지하고, 모든 전자서명에 **동등한 법적 효력 부여**
전자서명 이용자 보호	전자서명의 신뢰성 제고 및 이용자의 선택에 필요한 정보제공을 위해, 전자서명 인증업무 운영기준 **준수 사실 평가 · 인정제 도입**
경과조치	기존 공인인증서는 국민의 선택에 따라 계속 사용할 수 있도록 **경과조치 마련 등**

연관 법률

- 전자금융거래법
- 전자문서 및 전자거래기본법
- 정보통신망 이용촉진 및 정보 보호 등에 관한 법률
- 신용정보의 이용 및 보호에 관한 법률
- 전자금융감독규정
- 보험업법 시행령
- 상법
- 의료법
- 온라인투자연계금융업 및 이용자 보호에 관한 법률
- 대부업 등의 등록 및 금융 이용자 보호에 관한 법률

전자서명 시장의 변화

정부 중심의 공인인증제도 폐지

공인인증기관, PKI 기술기반의 보안 업체 주도의 본인인증 및 전자서명 기술

공인인증서의 독점적 법적지위 폐지

- 법적 효력의 우위로 인한 시장 독점의 문제 발생
- 사용자의 불편성 증대 및 지속적인 보안 취약점 발생

- 모든 전자서명에 동등한 효력을 부여하는 것으로 정책 전환
- 다양한 전자서명수단 활성화와 동시에 전자서명 이용자 보호 조치 강화

민간 중심의 자율 평가·인정 제도 시행

보안성과 편의성을 모두 충족시키는 사용자 & 서비스 중심으로 변화

민간의 다양한 전자서명인증사업자 출현

PASS, TALK, N, SAMSUNG Pass, PAYCO, KB 국민은행

- 민간 주도의 간편 전자서명 기술 개발이 활발하게 진행
- 이용기관의 다양한 전자서명수단 도입
- 대기업 중심의 시장주도로 중소기업의 시장진출 어려움 존재

다양한 전자서명인증서비스 확산 시작

다양한 전자서명인증서비스 출현으로 이용기관의 도입 부담 증가 & 국민불편 발생

상호연동 지원 필요성 대두

국세청 (행안부 시범사업) | 질병관리청 (백신예약) | 금융위원회 (마이데이터)

- 표준화 미비로 상호호환성 부재
- 보안성, 운영성에 대해 이용기관의 중복 검토 및 도입 비용 증가
- 이용기관의 신속한 적용 체계 지원 미비

시사점

전자서명법 개정으로 정부 중심에서 민간 주도로 제도 개편

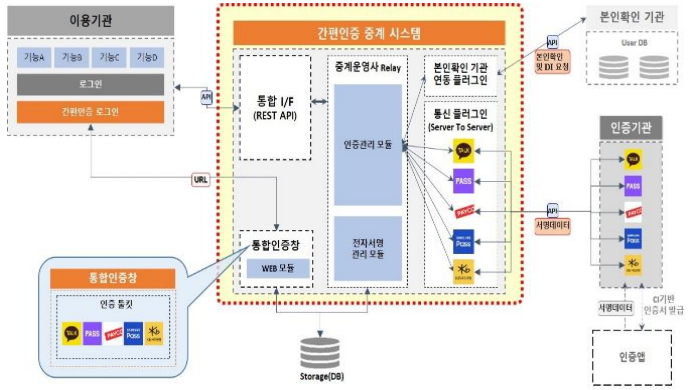
→ 다양한 민간 전자서명수단 출현 (18개, '22.8월 기준)

→ **다양한 전자서명인증서비스의 상호호환성 지원체계 필요성 대두**

국민의 다양한 전자서명수단 선택권 제공 방향

다양한 전자서명 적용사례

행정안전부

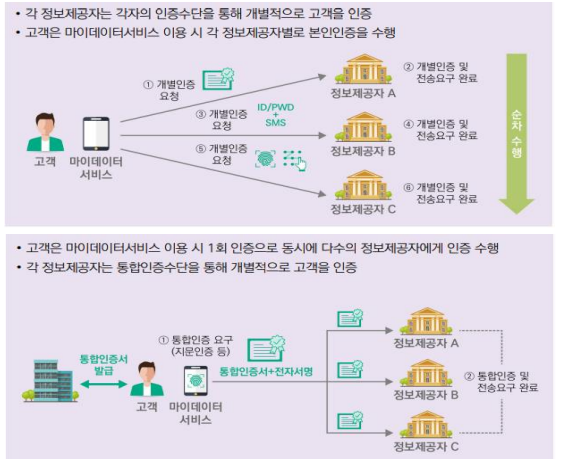


- 전자서명공통기반 사업을 통해 구현
- 중계 모듈의 개발 및 이용기관측에 배포하는 구조
  ※ 각 이용기관 측에 중계 모듈을 On-Premise 형태로 구축
- 중계 모듈에서 민간전자서명인증 사업자의 통신 규격을 개별로 구현하여 중계하는 방식

질병관리청

- COVID-19 백신 예약을 위한 사용자 확인
- 민간클라우드 내 다양한 사용자 확인 수단 중 하나로 사용
- 별도의 중계 모듈이 아닌, 각각의 민간전자서명인증 사업자와 직접 통신하는 형태로 구현

금융위원회



- 정보제공자별 개별 인증 또는 마이데이터 서비스에서 제공하는 통합 인증 사용 가능
- 전자서명법 개정의 취지에 부합하도록 다양한 전자서명 허용

시사점

통합된 중계모듈의 개발에도 전자서명인증사업자별 규격을 사용

→ 개별 분야에서 구축된 결과물을 타 분야에서 활용하지 못해 별도의 구축 및 테스트로 인한 중복투자 발생

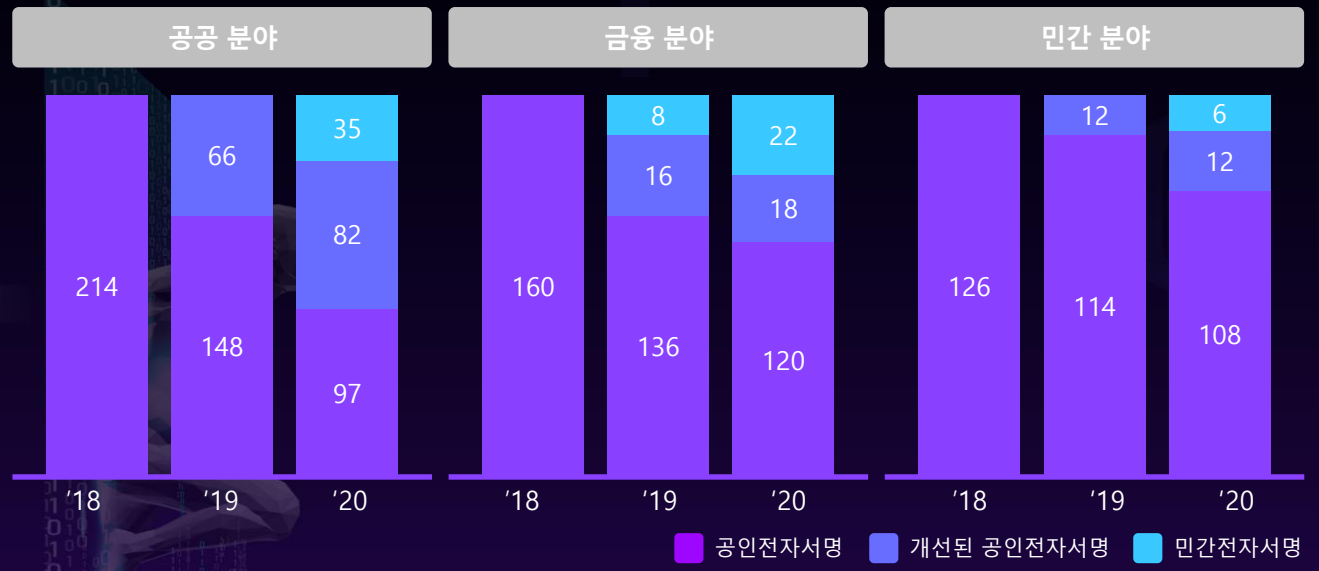
→ **이용기관의 검토 기간 단축 및 중복투자의 해결책 필요**

웹사이트 전자서명 이용현황

500개 웹사이트 전자서명 이용실태 조사 결과

구분		주요 서비스 분야	대상
공공	민원행정	연말정산, 정부민원, 부동산전자등기 등	205
	정부전자조달	전자조달, 전자입찰 등	9
금융	인터넷뱅킹	인터넷 은행거래, 은행 계좌관리 등	104
	인터넷증권	인터넷 증권거래, 증권 계좌관리 등	31
	인터넷보험/카드	보험상품 가입해지, 신용카드 신청해지 등	25
민간	전자상거래	신용카드 결제, 전자세금계산서, 휴대전화 개통 등	16
	온라인교육	대학 학사업무, 평생교육원 학사업무 등	66
	전자의료	전자처방전, 전자의무기록 등	44
총 서비스 분야			**500**

이용분야별 전자서명기술 도입 현황



- **공공 분야** | 정부주도 전자서명 공통기반 제공으로 민원행정서비스에서 도입 확산 추세
- 민원행정 205개, 전자조달 9개 사이트 중 민원행정서비스 35개에서 카카오페이, 패스 등의 간편인증서 도입

- **금융 분야** | 국민의 재산과 밀접한 관계로 다양한 전자서명수단 도입에 신중
- 인터넷뱅킹 104개, 증권 31개, 보험/신용카드 25개 중 22개 사이트에서 패스, 네이버 등의 민간 전자서명 도입

- **민간 분야** | 다양한 전자서명수단 확산체계 부재로 이용기관의 도입이 저조
- 전자상거래 16개, 온라인교육 66개, 전자의료 44개 중 6개 사이트에서 카카오, 네이버, 패스 등의 민간 전자서명 도입

[출처: 공인인증서 폐지에 따른 전자서명 이용 실태조사('20.12월, KISA)]

국민의 개선 요구사항

국민은 자신이 이용하고자 하는 전자서명수단이 다양한 홈페이지에서 지원되지 않아 불편을 호소하고 상호연동성*에 대한 개선을 요구

* 국민이 생각하는 상호연동성은 하나의 전자서명수단으로 다양한 홈페이지에서 이용 가능한 환경을 의미

국민은 다양한 전자서명수단(인증서)을 사용할 때 불편사항으로
"다양한 홈페이지에서 이용 불가능(37.1%)"한 점을 가장 높게 응답

구분	다양한 홈페이지에서 이용 불가능	안정적 서비스에 대한 의구심	전자서명인증서가 익숙치 않아서	인증서 종류가 많아서	기타
전체	37.1%	31.7%	25.7%	4.8%	0.6%
공공	43.2%	22.7%	31.8%	2.3%	0.0%
금융	42.2%	25.0%	26.6%	4.7%	1.6%
민간	27.1%	45.8%	20.3%	6.8%	0.0%

또한, 국민은 전자서명수단(인증서)을 선택할 때 고려하는 사항으로
"상호연동성(63.1%)"을 가장 높게 응답

구분		상호연동성	서비스안정성	이용편의성	다양한 이용처	이용비용
전체		63.1%	53.6%	44.3%	32.4%	6.7%
연령	10대	34.8%	63.0%	50.0%	32.6%	19.6%
	20대	65.1%	49.1%	47.1%	32.5%	6.2%
	30대	65.0%	50.1%	44.2%	34.6%	6.1%
	40대	62.5%	56.4%	41.4%	33.3%	6.4%
	50대	61.6%	55.7%	45.5%	30.6%	6.6%
	60대	65.6%	54.5%	44.3%	29.2%	6.3%

[출처: 전자서명법 개정에 따른 전자서명 이용 실태조사('21.12월, KISA)]

다양한 전자서명 상호연동 지원을 위한 정보화전략계획 수립

전자서명법 개정에 따른 다양한 방식의 전자서명 수단에 대한 상호호환성을 제공하기 위해 디지털인증 확산센터 구축 및 운영을 위한 정보화전략계획(ISP) 수립 추진('21.6월~11월)

■ 배경 및 목적

디지털인증 확산센터 구축 및 운영을 위한

정보화전략계획(ISP) 사업 추진

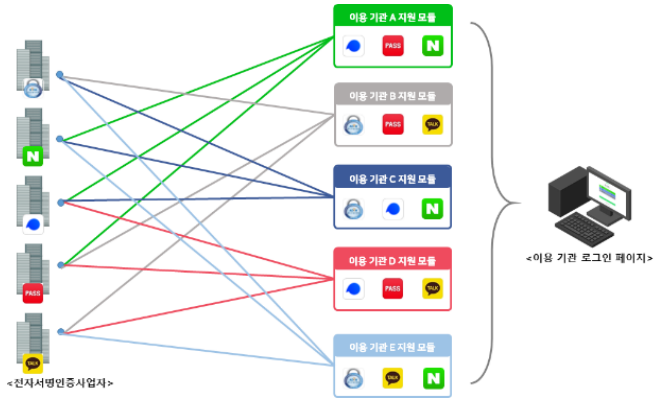
- 센터운영 최적화 프로세스 수립
- 다양한 전자서명 연동을 위한 기술 및 기반구조 수립
- 정보자원 관리체계 수립
- 목표 모델 구축 전략 수립

- 사용자 중심의 편의성 확보 및 동일한 서비스 경험을 제공
- 도입기관의 연동 편의성 확보로 전자서명 시장 활성화
- 각기 다른 전자서명 방식에 대한 이용기관의 연동 및 운영 부담 완화
- 다양한 전자서명 수단의 안정성, 편의성, 신뢰성 제고

다양한 전자서명수단 이용 활성화 방안 마련	● 전자서명법 개정 및 데이터 3법 개정, 공인인증서 제도 폐지로 전자서명수단 간 차별 없는 경쟁 환경 조성으로 디지털 인증 본격화로 전자서명 시장 재편 ● 전자서명인증사업자가 다양한 기술방식과 규격으로 전자서명을 개발 활용할 예정으로 상호호환성 문제우려
국민 편의성 제공을 위한 상호연동 지원체계 필요성 검토	● 신뢰성 있는 다양한 전자서명수단을 이용기관이 쉽게 적용하여 사용자에게 일관성 있고 편리한 전자서명서비스를 제공할 수 있는 효율적 환경 제공 필요
상호연동 지원에 따른 기대효과 분석	● 국민의 신뢰성 있는 다양한 전자서명수단 선택권 제공 ● 인증서, 생체인증(FIDO), 분산신원증명(DID) 등 다양한 전자서명서비스가 신뢰성있게 확산됨에 따른 이용기관 비용절감 효과 발생
디지털인증 확산센터 구축을 위한 계획 수립	● 상호연동지원센터 요구사항 도출 및 정의 ● 상호연동지원센터 기능 도출 및 업무프로세스 설계 ● 구축 및 운영을 위한 예산 수립

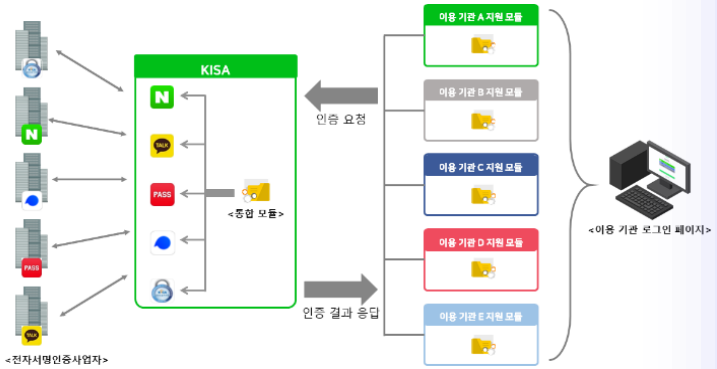
다양한 전자서명 상호연동 지원방안 비교

방안1 : 민간자율체계



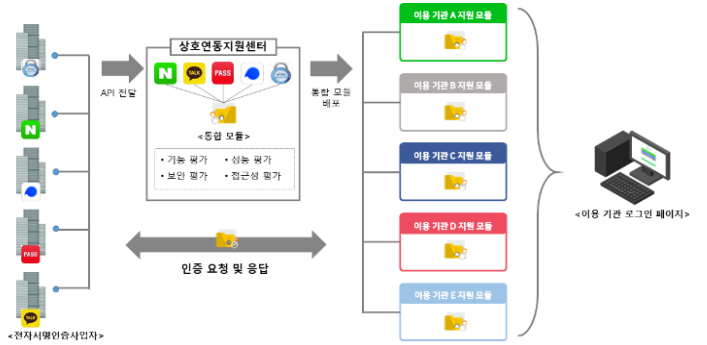
- 이용기관의 다양한 전자서명인증 수단 도입의 어려움
- 국민의 다양한 전자서명인증 수단의 선택권 제한
- 개별 전자서명인증사업자마다 상이한 인터페이스로 인해, 신규 적용 및 개별 협의에 대한 어려움 존재

방안2 : 중계서비스 제공 방식



- 이용기관과 서비스 사업자간 중간자 역할을 수행
- 통합 연동규격의 마련으로 신규 사업자 및 변경 사항에 대해 이용기관측의 최소화 변경
- 중계서비스는 대용량 트래픽 처리 및 안정성 문제 발생 시 싱글포인트 장애 문제점 존재
- 민간 중계서비스 시장에 대한 침해 소지 가능성 존재

방안3 : 통합 모듈 개발 및 관리



- 표준화된 통합 중계 모듈을 개발 · 검증하여 제공
- 기능구현 적합성 평가, 보안취약점 점검 등에 대한 사전검증으로 신뢰서비스의 품질을 보장
- 이용기관과 서비스 사업자간의 요구 사항 및 분쟁 상황 시, 중간자 역할을 수행
- 개별 신규 인프라 구축에 비해 사회적비용 절감 효과

시사점

이용기관의 도입 편의성,
운영용이성, 신뢰서비스 관점

→

국민의 다양한 전자서명수단
선택권 제공 강화 관점

→

방안3 통합 전자서명모듈
지원 및 관리 체계 중심으로 진행

다양한 전자서명 상호연동 지원 추진전략

VISION

신뢰성이 보장된 다양한 전자서명수단 선택권 제공으로 국민 편의성 제고 및 안전한 전자서명 시장 조성

구현방안

- 디지털인증 확산센터 신규 구축을 위한 방안 마련
- 이용기관 및 전자서명인증사업자의 참여를 위한 신청 절차 마련
- 통합 전자서명모듈의 보안성 점검을 위한 절차 및 환경 구축 방안 마련
- 통합 전자서명모듈의 각종 편의성 확보를 위한 절차 및 시험환경 구축
- 통합 전자서명모듈의 신뢰성 있는 배포 및 관리 방안 마련

추진방향

신뢰성이 검증된 다양한 전자서명수단 선택권 제공을 위한 디지털인증 확산센터 구축

표준화 수립 및 통합 전자서명모듈의 개발 및 관리를 통해 검증된 서비스를 이용기관 측에 제공

지속적인 배포 및 관리 체계 마련

추진전략

1. 신뢰된 전자서명인증 서비스를 위한 표준화 정립 및 검증을 위한 체계 마련
2. 이용기관 및 전자서명인증사업자의 참여를 위한 협의 및 검증환경 구성

1. 표준화 수립 및 준수여부를 검증하여, 범용성이 보장된 통합 모듈을 개발
2. 보안성 점검 및 이용성을 검증하여 이용기관의 도입 편의성을 제공
3. 통합 전자서명모듈 제공을 통한 신규 사업자의 시장진입 장벽을 해소

1. 이용기관의 참여 및 승인 절차를 위한 자동화 시스템 구축 · 운영
2. 효율적인 운영환경을 위해 배포 체계 및 장애 관리체계를 마련

국민의 다양한 전자서명수단 선택권 제공 방향

디지털인증 확산센터 주요 역할

전자서명법 개정으로 민간 중심의 다양한 전자서명인증서비스 출현

전자서명인증업무 운영기준 준수사실 평가 · 인정제도를 통해,
다양한 전자서명인증서비스에 대한 안전성 · 신뢰성 확보

안전성과 신뢰성이 확보된 다양한 전자서명인증서비스를 통합 개발하여
차별 없는 경쟁환경을 조성하고 국민의 전자서명 선택권을 강화

디지털인증 확산센터의 주요업무 정의

- 전자서명인증 기술 통합 전자서명모듈 개발
- 전자서명인증 기술 구현 적합성 평가
- 개발된 통합 전자서명모듈의 보안성과 안전성 검증
- 통합 전자서명모듈의 성능 및 부하 시험
- 웹 표준 적합성 점검
- 인증 절차 및 사용자 인터페이스의 표준화

표준화 및 개발

- **표준화를 위한 협의체 구성 및 운영**
  - 표준화 협의체 및 분과별 운영지원
  - 전자서명 이용분야 도입 및 확산을 위한 활동
  - 이용기관, 전자서명인증사업자, 사용자 불편 수렴 및 개선활동
- **표준화 인터페이스 개발**
  - 사용자에게 친숙하고 직관적인 인터페이스
- **배포용 라이브러리 개발**
  - 성능 및 보안성 검증이 완료되고, 손쉬운 연동성을 제공하는 라이브러리 개발

기능성 및 보안성 점검

- **테스트랩 운영**
  - 전자서명서비스의 기능구현 적합성, 상호연동 시험 등 사전 점검
- **기능/성능/보안성 테스트**
  - 웹 표준 적합성 점검, 성능 · 부하 시험, 보안 취약점 점검

배포체계

- **실시간 배포체계 지원**
- **이용기관 대상 매뉴얼 발행**
  - 전자서명 라이브러리 도입 및 적용을 위한 이용기관용 적용 매뉴얼 지원
- **상호연동 지원 및 컨설팅 수행**
  - 전자서명인증사업자-이용기관간 서비스 적용을 위한 안내 및 지원

이용기관협약

- **이용기관 신청 및 승인 체계**
- **이용기관 코드 및 접근 키 생성, 관리 지원**

장애관리

- **장애 내역 수집 및 분석**
  - 인증 건수 및 오류내역 분석, 통계
- **이용기관과 전자서명인증사업자간 중간자 역할**

국민의 다양한 전자서명수단 선택권 제공 방향

디지털인증 확산센터 구축 방안

다양한 전자서명수단 확산 시범지원 사업 추진

■ 다양한 전자서명수단 확산 시범지원(40개 이용기관)

향후 추진계획

디지털인증 확산센터 구축과 운영을 위한 통합 이행계획 수립 및 실행

추진 단계	1단계: 디지털인증 확산센터 신규 구축 및 시범운영 (2023년)	2단계: 디지털인증 확산센터 정식 운영 및 확산 (2024년)	3단계: 디지털인증 확산센터 신기술 확대 및 고도화 (2025년)
주요 내용	**시범 운영 단계** 디지털인증 확산센터를 신규 구축하고 운영하기 위한 기반을 만들고 시범 서비스를 제공하는 단계	**서비스 확산 단계** 디지털인증 확산센터 시범 운영 결과를 기반으로 도출된 개선사항을 반영하여 이용기관 적용을 확산하고 안정적으로 센터를 운영하는 단계	**시스템 고도화 단계** X.509 기반 전자서명인증 기술과 더불어 DID 등의 신기술 적용을 통한 디지털인증 확산센터 내 시스템 고도화 단계
추진 방향	• 디지털인증 확산센터 신규 구축 • 전자서명인증 모듈 및 UI 통합 개발 • 통합 모듈 기능구현적합성 평가, 성능 · 부하 점검, 보안성 검증 등을 위한 테스트 랩 구축 • 시범 운영을 통한 개선사항 도출 및 개선방안 마련	• 디지털인증 확산센터 시스템 안정화 • 다양한 전자서명수단 확대 적용 • 이용기관 참여 확대 • 서비스 확산, 신기술 도입 등을 위한 디지털인증확산센터 고도화 계획수립	• 통합 모듈에 대한 성능 및 지원 범위 개선을 위한 시스템 고도화 • 이용기관 확대로 인한 설비 고도화 • 분산신원증명 등 신기술 적용 • 트러스트앵커 체계 구축방안 마련 • 민간 디지털지갑 지원방안 마련

기대 효과

1 국민 관점

- 다양한 전자서명수단 통합 제공으로 사용자의 다양한 전자서명인증서비스 선택권 강화
- 기능, UI/UX의 표준화를 통한 사용자의 전자서명인증서비스 이용혼란 감소
- 안전성과 신뢰성이 검증된 서비스 제공으로 사용자의 전자서명인증서비스 안전성 강화

2 이용기관 관점

- 다양한 전자서명인증서비스 개발 및 연동에 소모되는 비용 감소
- 다양한 전자서명인증서비스 신속 적용 가능
- 사용자에게 안전하고 신뢰성 있는 전자서명인증서비스 제공
- 사용자에게 동일한 기능 및 이용 환경 제공을 통한 편의성 개선

3 인정사업자 관점

- 디지털인증 확산센터에 참여하는 이용기관에 전자서명인증서비스 확산
- 개별 연동으로 인해 발생하는 유지보수, 적용지원 등의 소모 비용 감소
- 다양한 전자서명인증사업자의 차별 없는 공정경쟁 환경 마련

시큐업 세미나 2022

디지털 인증의 현재와 미래

토스인증서

본인확인이 필요한 모든 순간

토스 **방승익 실장**

2022.10.04

본인확인 / 전자서명

본인확인

본인확인기관으로써 고객의 연계정보 수집을 위한 연계정보(CI,DI)를 처리(제공)할 수 있는 서비스

「전자서명법」 제8조에 따라 운영기준 준수 사실의 인정을 받은 전자서명인증사업자

전자서명

toss

토스인증서 3대 강점 (토스인증서를 왜 써야 할까요?)

1 공동인증서와 동일한 효력을 인정받아 보유하고 있는 사설 인증서입니다

- 본인확인기관(21년 8월) 및 전자서명인증사업자(21년 11월) 라이센스를 모두 보유 중인 유일한 사설인증서로 공인인증서와 동일한 효력을 보유

2 토스인증서 도입 기관 및 이용자 모두에게 차별화된 유저 경험을 제공합니다

- 기관: 간단한 절차, 체계적인 가이드, 빠른 이슈대응으로 7 영업일 내 서비스 연동 가능 / 이용자: 번거로운 다단계 인증 절차를 원터치로 한 번에 완료

3 토스인증서 하나로 금융/공공/일반 기관들의 모든 인증 수요를 충족할 수 있습니다

- 간편인증, 본인확인, 전자서명, 마이데이터통합인증 서비스를 이용하여 회원가입/로그인에서부터 각종 동의문 서명까지 모든 인증 수요 커버 가능

토스인증서 3대 강점 (토스인증서를 왜 써야 할까요?)

1 공동인증서와 동일한 효력을 인정받아 보유하고 있는 사설 인증서입니다

- 본인확인기관(21년 8월) 및 전자서명인증사업자(21년 11월) 라이선스를 모두 보유 중인 유일한 사설인증서로 공인인증서와 동일한 효력을 보유

2 토스인증서 도입 기관 및 이용자 모두에게 차별화된 유저 경험을 제공합니다

- 기관: 간단한 절차, 체계적인 가이드, 빠른 이슈대응으로 7 영업일 내 서비스 연동 가능 / 이용자: 번거로운 다단계 인증 절차를 원터치로 한 번에 완료

3 토스인증서 하나로 금융/공공/일반 기관들의 모든 인증 수요를 충족할 수 있습니다

- 간편인증, 본인확인, 전자서명, 마이데이터통합인증 서비스를 이용하여 회원가입/로그인에서부터 각종 동의문 서명까지 모든 인증 수요 커버 가능

1. 사설인증서로는 유일하게 공동인증서와 동일한 효력

토스인증서는 관련 법령 및 제도적 요건을 모두 준수하는 인증서입니다

전자서명법

과학기술정보통신부
Ministry of Science and ICT

전자서명인증사업자 인정평가제도

2021년 11월 전자서명인증사업자로
인정받아 사설인증 서비스 제공

정보통신망법

방송통신위원회
Korea Communications Commission

방송통신위원회 지정 본인확인기관

2021년 8월 본인확인기관으로 지정되어
본인확인서비스 제공 (저장 가능한 CI, DI 제공)

전자금융거래법 및 신용정보법

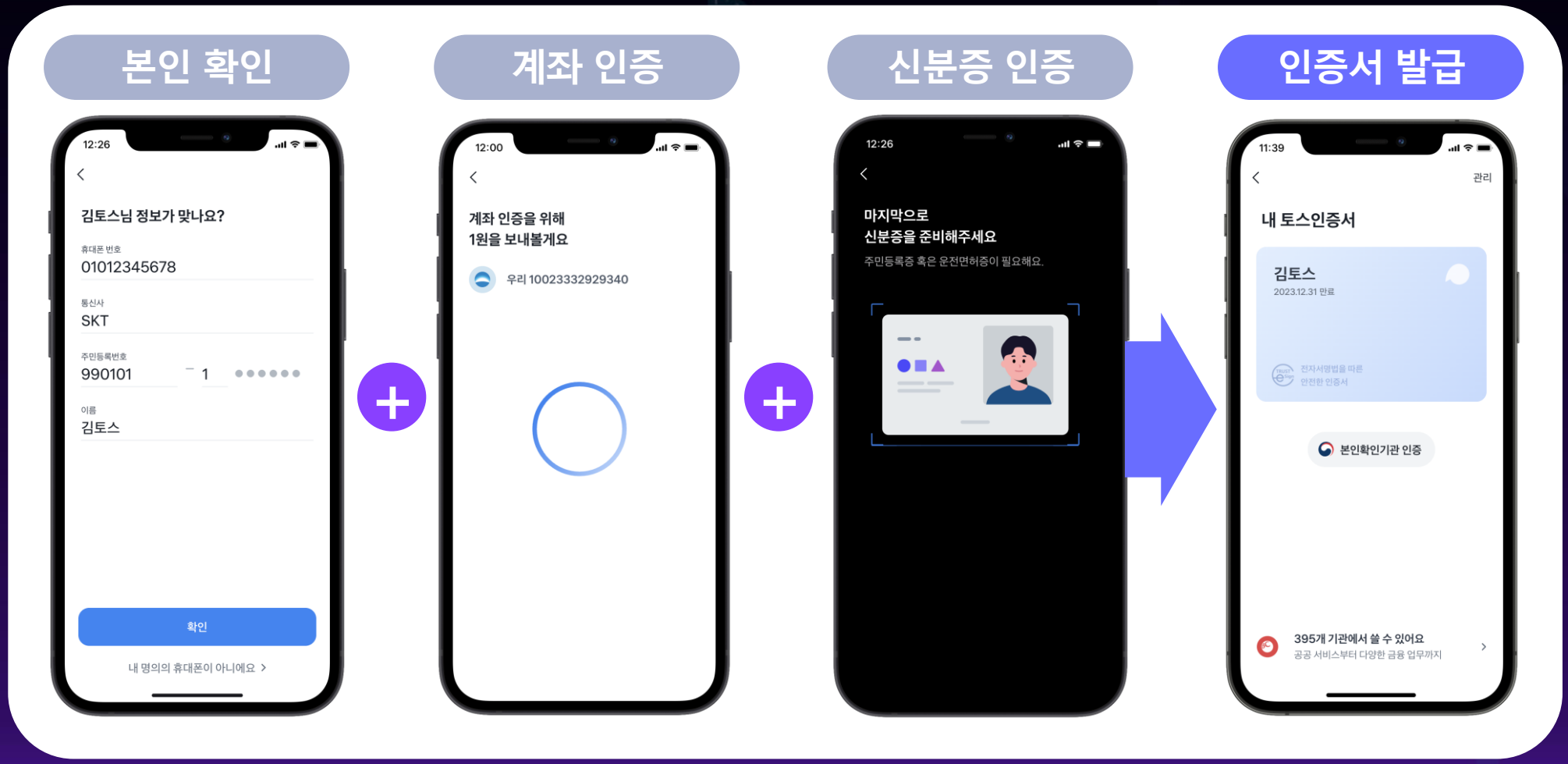
금융위원회
Financial Services Commission

**비대면 금융거래 및 마이데이터
서비스를 위한 통합 인증수단**

2021년 12월 통합인증기관으로 지정되어
마이데이터 사업자를 위한 통합인증 제공

1. 사설인증서로는 유일하게 공동인증서와 동일한 효력

토스인증서는 비대면 실명확인 단계 거쳐 실지명의[1]를 확인한 뒤 발급합니다

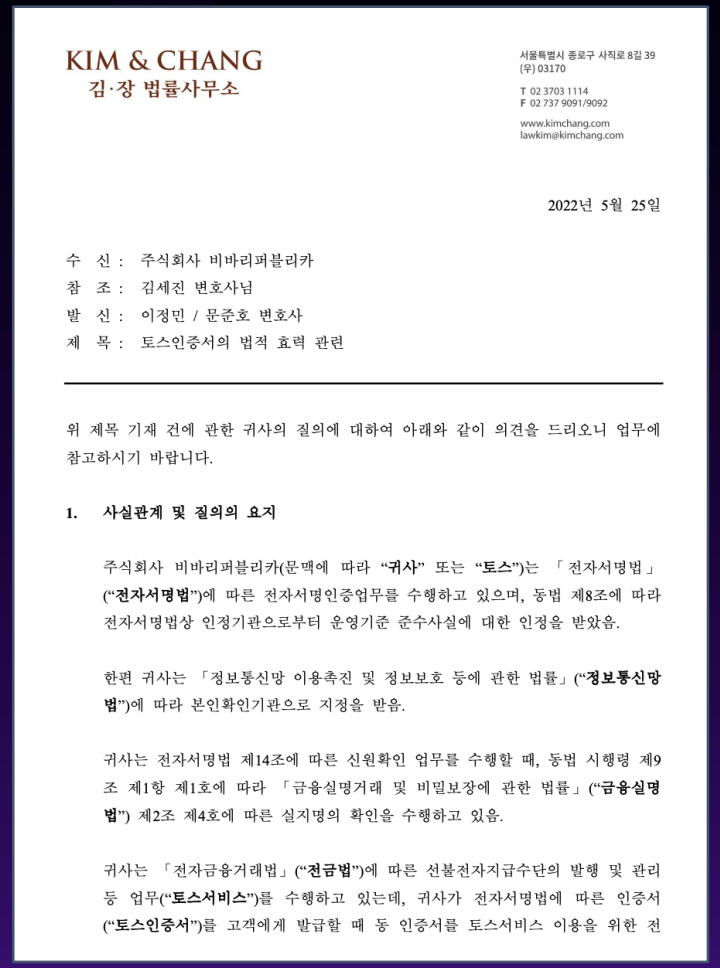


1)실지명의란 주민등록증 또는 운전면허증 등 정부가 공인한 신분증 상의 이름과 주민등록번호를 말함

본인확인이 필요한 모든 순간, 토스인증서

1. 사설인증서로는 유일하게 공동인증서와 동일한 효력

토스인증서는 공동인증서와 동일한 효력을 가집니다 (참고자료: 김앤장 법률 의견서)



KIM & CHANG
김·장 법률사무소

서울특별시 종로구 사직로 8길 39
(우) 03170

T 02 3703 1114
F 02 737 9091/9092

www.kimchang.com
lawkim@kimchang.com

2022년 5월 25일

수 신 : 주식회사 비바리퍼블리카
참 조 : 김세진 변호사님
발 신 : 이정민 / 문준호 변호사
제 목 : 토스인증서의 법적 효력 관련

위 제목 기재 건에 관한 귀사의 질의에 대하여 아래와 같이 의견을 드리오니 업무에 참고하시기 바랍니다.

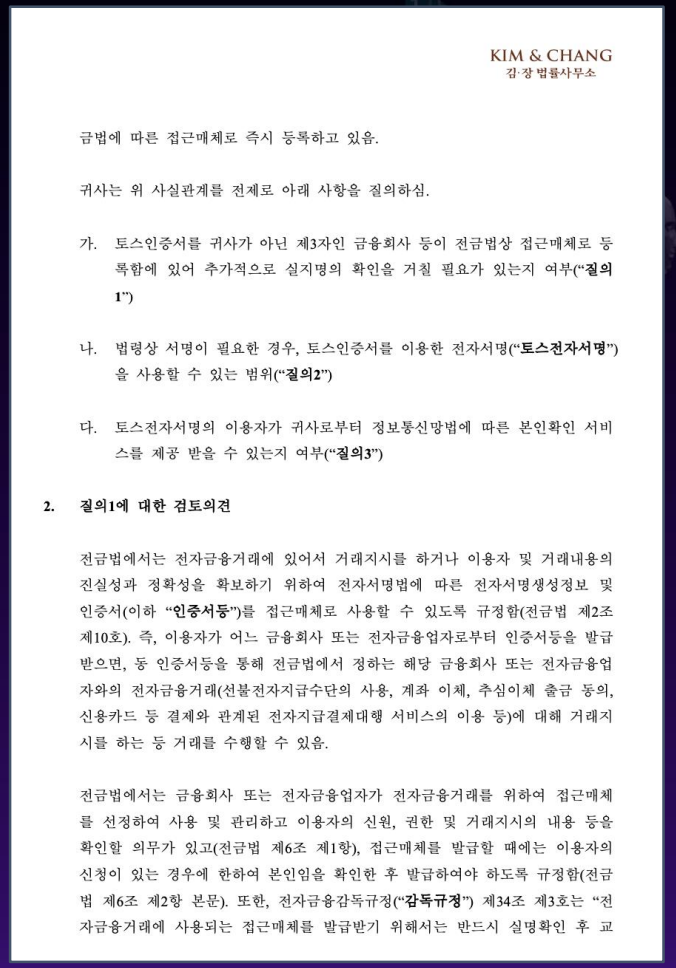
1. 사실관계 및 질의의 요지

주식회사 비바리퍼블리카(문맥에 따라 **"귀사"** 또는 **"토스"**)는 「전자서명법」(**"전자서명법"**)에 따른 전자서명인증업무를 수행하고 있으며, 동법 제8조에 따라 전자서명법상 인정기관으로부터 운영기준 준수사실에 대한 인정을 받았음.

한편 귀사는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(**"정보통신망법"**)에 따라 본인확인기관으로 지정을 받음.

귀사는 전자서명법 제14조에 따른 신원확인 업무를 수행할 때, 동법 시행령 제9조 제1항 제1호에 따라 「금융실명거래 및 비밀보장에 관한 법률」(**"금융실명법"**) 제2조 제4호에 따른 실지명의 확인을 수행하고 있음.

귀사는 「전자금융거래법」(**"전금법"**)에 따른 선불전자지급수단의 발행 및 관리 등 업무(**"토스서비스"**)를 수행하고 있는데, 귀사가 전자서명법에 따른 인증서(**"토스인증서"**)를 고객에게 발급할 때 동 인증서를 토스서비스 이용을 위한 전



KIM & CHANG
김·장 법률사무소

금법에 따른 접근매체로 즉시 등록하고 있음.

귀사는 위 사실관계를 전제로 아래 사항을 질의하심.

가. 토스인증서를 귀사가 아닌 제3자인 금융회사 등이 전금법상 접근매체로 등록함에 있어 추가적으로 실지명의 확인을 거칠 필요가 있는지 여부(**"질의1"**)

나. 법령상 서명이 필요한 경우, 토스인증서를 이용한 전자서명(**"토스전자서명"**)을 사용할 수 있는 범위(**"질의2"**)

다. 토스전자서명의 이용자가 귀사로부터 정보통신망법에 따른 본인확인 서비스를 제공 받을 수 있는지 여부(**"질의3"**)

2. 질의1에 대한 검토의견

전금법에서는 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 전자서명법에 따른 전자서명생성정보 및 인증서(이하 **"인증서등"**)를 접근매체로 사용할 수 있도록 규정함(전금법 제2조 제10호). 즉, 이용자가 어느 금융회사 또는 전자금융업자로부터 인증서등을 발급받으면, 동 인증서등을 통해 전금법에서 정하는 해당 금융회사 또는 전자금융업자와의 전자금융거래(선불전자지급수단의 사용, 계좌 이체, 추심이체 출금 동의, 신용카드 등 결제와 관계된 전자지급결제대행 서비스의 이용 등)에 대해 거래지시를 하는 등 거래를 수행할 수 있음.

전금법에서는 금융회사 또는 전자금융업자가 전자금융거래를 위하여 접근매체를 선정하여 사용 및 관리하고 이용자의 신원, 권한 및 거래지시의 내용 등을 확인할 의무가 있고(전금법 제6조 제1항), 접근매체를 발급할 때에는 이용자의 신청이 있는 경우에 한하여 본인임을 확인한 후 발급하여야 하도록 규정함(전금법 제6조 제2항 본문). 또한, 전자금융감독규정(**"감독규정"**) 제34조 제3호는 "전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교

공동인증서(구 공인인증서)와 동일한 지위

토스는 정보통신망법상 본인확인 업무와
전자서명법상 전자서명인증 업무 모두 수행 가능함
(구 공인인증서 사업자와 동일한 지위 보유)

본인확인서비스 기반의 본인인증 제공

이용기관이 필요한 경우 토스로부터 제공받은
연계정보(CI) 및 중복가입정보(DI)는 저장 가능함
(일반 간편인증 기관이 제공하는 CI는 저장 불가)

타 전자서명보다 안전하고 보안성 강함

구 공인인증서와 같은 효력이 있으므로
타 전자서명보다 안전하고 보안성이 강한
전자서명을 발급 · 관리 · 이용한다고 볼 수 있음

참고: 의견서의 요지는 가) 토스인증서의 권능을 고려할 때 전금법상 접근매체로 등록함에 있어 추가 실지명의 확인이 필요 없음, 나) 법령상 규정하는 전자서명 모두에 사용할 수 있음, 다) 정보통신방법에 따른 본인확인서비스를 제공 받을 수 있음
출처: 김앤장 법률 의견서 (2022년 5월)

토스인증서 3대 강점 (토스인증서를 왜 써야 할까요?)

1 공동인증서와 동일한 효력을 인정받아 보유하고 있는 사설 인증서입니다

- 본인확인기관(21년 8월) 및 전자서명인증사업자(21년 11월) 라이센스를 모두 보유 중인 유일한 사설인증서로 공인인증서와 동일한 효력을 보유

2 토스인증서 도입 기관 및 이용자 모두에게 차별화된 유저 경험을 제공합니다

- 기관: 간단한 절차, 체계적인 가이드, 빠른 이슈대응으로 7 영업일 내 서비스 연동 가능 / 이용자: 번거로운 다단계 인증 절차를 원터치로 한 번에 완료

3 토스인증서 하나로 금융/공공/일반 기관들의 모든 인증 수요를 충족할 수 있습니다

- 간편인증, 본인확인, 전자서명, 마이데이터통합인증 서비스를 이용하여 회원가입/로그인에서부터 각종 동의문 서명까지 모든 인증 수요 커버 가능

2. 이용기관/이용자 모두에게 차별화된 유저 경험

원터치 인증: 인증 절차를 1~2 단계로 끝내는 차별화된 경험을 제공합니다

[예시] Mobile 토스 본인인증 프로세스

Mobile
본인인증
인증 퍼널

토스인증 선택 | PIN or 생체인증 | 인증완료

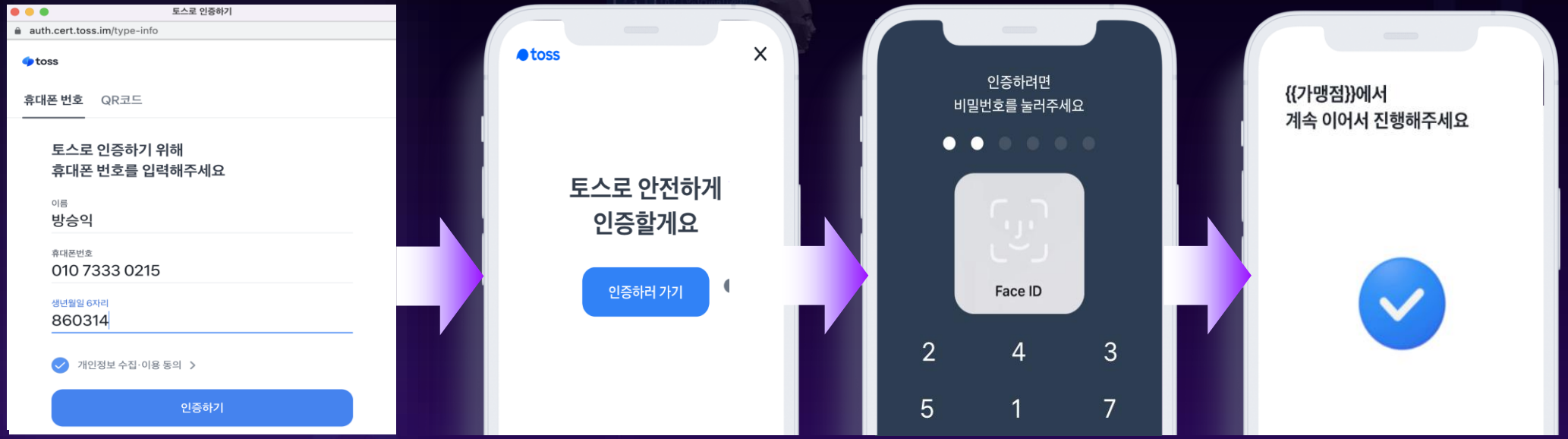
[이용기관] 서비스 사용 퍼널을 간소화할 수 있어 유저의 이탈율을 낮추고 전환율을 높임
[이용자] API 기반 연동을 통해 개인정보 입력 및 약관 동의 없이 PIN or 생체인증만으로 인증 절차 완료

2. 이용기관/이용자 모두에게 차별화된 유저 경험

Web 인증: 인증 절차를 간소화하여 차별화된 경험을 제공합니다

[예시] Web 토스 본인인증 프로세스

Web 본인인증 인증 퍼널



개인정보 입력(3개) → 토스인증 선택 → PIN or 생체인증 → 인증완료

[이용기관] 서비스 사용 퍼널을 간소화할 수 있어 유저의 이탈율을 낮추고 전환율을 높임
[이용자] API 기반 연동을 통해 개인정보 입력 및 약관 동의 없이 PIN or 생체인증만으로 인증 절차 완료

토스인증서 3대 강점 (토스인증서를 왜 써야 할까요?)

1 공동인증서와 동일한 효력을 인정받아 보유하고 있는 사설 인증서입니다

- 본인확인기관(21년 8월) 및 전자서명인증사업자(21년 11월) 라이센스를 모두 보유 중인 유일한 사설인증서로 공인인증서와 동일한 효력을 보유

2 토스인증서 도입 기관 및 이용자 모두에게 차별화된 유저 경험을 제공합니다

- 기관: 간단한 절차, 체계적인 가이드, 빠른 이슈대응으로 7 영업일 내 서비스 연동 가능 / 이용자: 번거로운 다단계 인증 절차를 원터치로 한 번에 완료

3 토스인증서 하나로 금융/공공/일반 기관들의 모든 인증 수요를 충족할 수 있습니다

- 간편인증, 본인확인, 전자서명, 마이데이터통합인증 서비스를 이용하여 회원가입/로그인에서부터 각종 동의문 서명까지 모든 인증 수요 커버 가능

3. 금융/공공/일반 영역 내 모든 인증 수요 충족

토스인증서 하나로 금융/공공/일반 영역 내 모든 인증 수요를 충족합니다

	간편인증/본인확인	전자서명	마이데이터 통합인증
서비스 설명	• 이용자 신원을 본인확인시스템을 통해 확인 후 **저장 가능한 CI/DI 제공** • 토스 본인인증은 **휴대폰 본인확인 및 일반 간편인증 서비스를 포괄**함	• 각종 전자문서 및 전자계약서와 관련한 **서명 기능 제공** • 계약 등 기록 에 대한 **부인방지**, 약관 등 **내용 확인에 대한 증빙**으로 사용	• **마이데이터** 사업자 및 정보제공자 기관을 위한 **통합인증 제공**
도입 사례	• 회원가입, 로그인, 가입조회 • 아이디/비밀번호 찾기 • (송금, 결제) 사용자 2차 인증 • 각종 본인확인 • 성인인증 • 행정안전부 간편인증 등	• 계좌, 증권 개설, 비대면 계좌 개설 등 • 각종 계약서/청구서 등 문서 전자서명 • 안내문, 수취확인 등 문서 전자서명 • 금융(자동)이체 동의 (예: 예적금, 보험 등) • 기부금 자동이체 동의 • 출금이체 동의 • 상품가입/권유에 대한 동의 등	• 기관별 마이데이터 서비스 가입

3. 금융/공공/일반 영역 내 모든 인증 수요 충족

특히 금융사들의 다양한 전자서명 수요는 더욱 완벽하게 충족시킵니다

은행 /저축은행

보험

카드

증권

	은행 /저축은행	보험	카드	증권
계약체결	• 주택담보 대출계약 • 신용대출 계약	• 보험가입설계동의 • 보험계약	• 신용카드 발급	• 증권신탁계약
접근매체	• 계좌이체	• 계좌이체	• 신용카드/직불카드 결제 • 선불전자지급 수단 이용	• 주식매매
추심이체 출금동의	• 대출원리금 납부 • 계좌설정	• 대출원리금 납부 • 계좌설정	• 카드대금 납부계좌 설정 • 선불전자 지급수단 충전	• 오픈뱅킹 서비스 • 계좌 설정
금소법상 고객확인	• 주택담보대출신청 • 신용대출신청	• 보험가입 • 보험대출신청	• 신용카드 신청	• 증권계좌 개설
마이데이터 서비스	마이데이터 통합인증			

참고: 금융소비자보호법 제17조 에 따라 소비자에게 금융상품 계약체결 할 때 뿐만 아니라 설명 및 권유 시에도 날인 및 전자서명이 필요함

토스인증서가 탑재된 토스앱은 국내에서 가장 안전한 금융 서비스입니다

ISO/IEC 27001

- 2017년 5월 취득 (2020년 4월 갱신 심사 완료)
- 국제표준화기구(ISO) 및 국제전기기술위원회(IEC)가 제정하는 **국제 표준 규격**
- 정보보호 정책, 물리적 보안, 정보접근 통제 등 정보보호 관리 기준에 따른 심사를 통과한 기업에 부여

PCI DSS Level 1

- 2017년 12월 취득
- 글로벌 카드사 5개가 정보 보안을 강화하기 위한 협의회를 설립해 개발한 **국제 보안 표준 규격**
- 총 6개 영역 415개 세부 요건에 대한 평가를 거쳐 최고 등급인 Level 1 취득

ISMS-P

- 2022년 1월 취득
- 과학기술정보통신부가 주관하는 **국내 최고 수준**의 종합 정보보호 및 개인정보 관리체계 인증제도
- 기업의 정보보호 및 개인정보 관리체계 적합 여부를 102개 인증 기준에 따라 한국인터넷진흥원이 심사 후 인증

ISO/IEC 27701

- 2020년 4월 취득
- **국제 표준** 개인 정보 보호 관리체계 인증
- 총 8개 분야, 49개의 관리 기준에 걸쳐 유럽 개인정보보호법의 가이드라인에 부합해야 취득

시큐업 세미나 2022

디지털 인증의 현재와 미래

Digital Transformation with NAVER

사용자를 사로잡는 디지털 전략

네이버 주식회사 **최욱동 리더**

2022.10.04

#Digital #User #Lock-in

How

사이트 방문

회원가입

- 회원가입여부 확인
- 회원정보 입력
- 본인인증

사이트 탐색

서비스 이용

계약 및 구매

- 프로그램 설치
- 인증서 등록
- 인증서 인증

서비스 이용 종료

재계약 or 타사 서비스 계약

사이트 방문

원클릭 회원가입

사이트 탐색

원클릭 계약

서비스 이용

서비스 관련 안내

원클릭 재계약

충성 고객화

#5,400만
회원

#No.1
포털

#광고,
페이, 쇼핑
연계

#MAU
4,000만

#빅테크
1st
인증평가
획득

#No.1
처리능력

N 인증서

#네이버
주식회사

#금융기관
80% 적용

NAVER BUSINESS FLOW

5천만 회원과 일일 3,000만 순방문이 이뤄지는 네이버 플랫폼을 기반으로
회원가입부터 인증, 증빙, 결제, 고객관리까지!

디지털 비즈니스의 흐름이 끊기지 않게 이어주는 종합 솔루션을 제시합니다.

회원가입

로그인 /
출입

본인 인증

증명 /
전자서명

결제

알림/공지
(고객관리)

500여 곳의 공공 / 금융 / 민간기관이 네이버와 디지털 전략을 함께하고 있습니다.

공공기관	행정안전부 간편인증을 통한 70여 공공기관, 국민연금공단, SH공사, LH공사, 한국부동산원, 한국자산관리공사, 대한법률구조공단, 한국도로공사, 국세청, 정보통신진흥협회, 질병청, 한국문화예술위원회, 서울시 복지포털 등 다수의 공공 기관
금융기관	W은행, D은행, S은행, I은행, D손보, N손보, H손보, C손보, H화재, H생명, M화재, M손보, H화재, K생명, K증권, S투자, M증권, B캐피탈, M캐피탈, H캐피탈, W저축은행 등 다수의 금융 기관
통신 및 생활서비스	K통신, L통신, S통신, C통신, M통신, H백화점, L백화점, E마트, K사이버대, Y대, G사이버대 등 다수의 민간 기관
금융 마이데이터	60여 마이데이터 사업자의 대부분이 네이버 인증서를 채택, 50개 금융/핀테크/통신사들의 마이데이터 통합인증 서비스 중

네이버 디지털 파트너를 위한 이벤트

시큐업 세미나 2022

디지털 인증의 현재와 미래