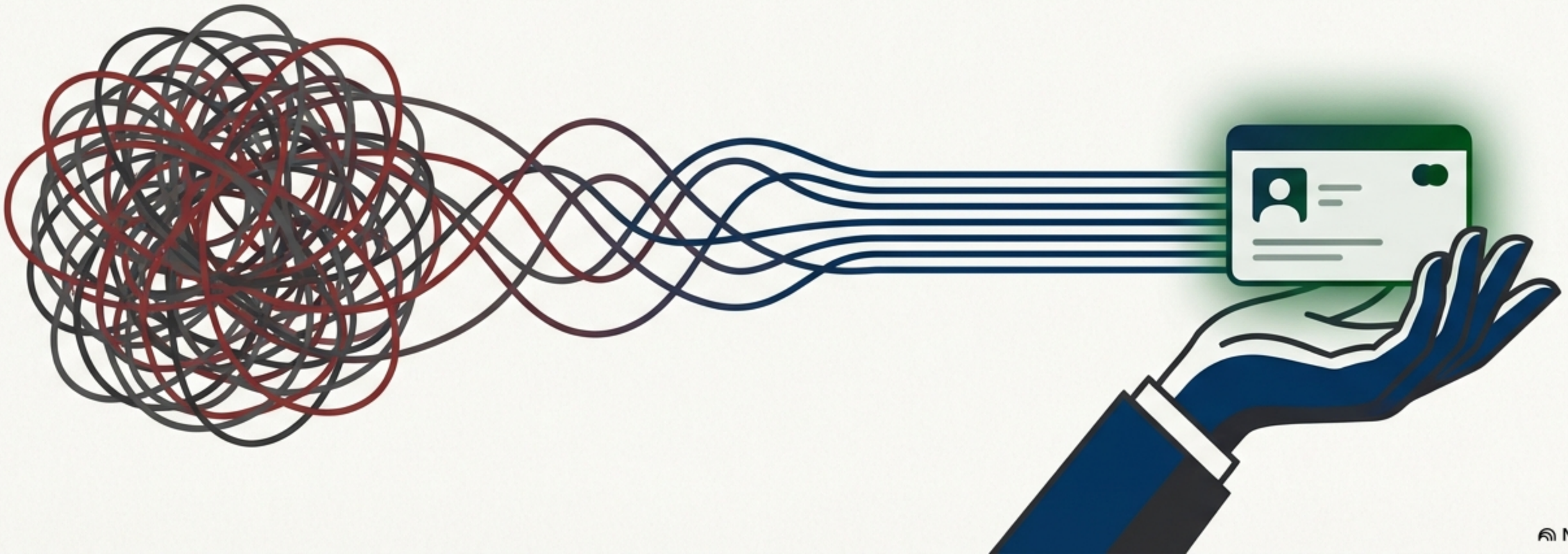
디지털 신원: 통제권을 되찾을 시간

대한민국 민간 본인확인 체계의 문제점에서
모바일 신분증과 eIDAS 2.0의 새로운 패러다임까지



우리의 본인확인, 과연 누구를 위한 것이었을까요?

국가 🇰🇷

국민 👤

본인확인은 중요합니다.
그래서 민간의 전문성을 활용했습니다.

전문성이라기엔…
CI 만들어서 중계한 게 핵심이었죠?

민간이 있어서 서비스가
빠르게 확산됐습니다.

왜 그 과정에서 국민 식별자가
민간의 핵심 자산이 됐죠?

주민등록번호를 대체하려다 '온라인 주민등록번호'를 만들었습니다

CI (연계정보)

한 사람에게 평생 할당되는 88바이트의 고유 식별자.
모든 서비스에서 동일하며, 주민등록번호와 1:1 매핑되어
'온라인 주민등록번호'로 기능합니다.

DI (중복가입확인정보)

웹사이트별로 발급되는 64바이트 식별자.
특정 사이트 내 중복 가입을 방지하는 데 사용됩니다.

핵심 문제 (Key Insight)

주민등록번호 수집을 막기 위해 설계된 시스템이,
결국 소수 민간 기업이 통제하는 새로운 형태의 보편적 추적 장치를 만들었습니다.

'검증'이 아닌 '연결'에 집중한 시스템: 사용자는 통제권을 잃었습니다

개인 식별 및 추적 (Personal Identification & Tracking)

CI는 보편적이므로, 기업들은 여러 서비스에 걸친 사용자의 활동을 연결하고 추적할 수 있습니다.

사용자 통제권 부재 (Lack of User Control)

사용자는 CI가 유출되어도 변경을 요청할 수 없으며, 발급이나 폐기 과정에 아무런 권한이 없습니다.

법적 보호 미비 (Insufficient Legal Protection)

DI는 법적으로 명확히 보호되지 않아, 영장 없이도 개인의 웹사이트 가입 내역을 추적할 수 있는 허점이 존재합니다.

국제 호환성 제로 (Zero Global Compatibility)

주민등록번호에 종속된 한국만의 독특한 구조로, 외국인 사용이 어렵고 글로벌 표준과 호환되지 않습니다.

본인확인은 보안 산업이 아니라 ‘법으로 만든 통행료 산업’이었습니다

“보안이라면 왜 ‘연결(CI)’이 중심이고 ‘검증’은 부차적이었죠?
...국가 신분증은 되는데, 왜 민간 본인확인은 아직도 식별자 장사 구조여야 하죠?”

핵심 비즈니스 모델은 보안 강화가 아니라,
법적으로 보장된 신원 연결 독점권을 통해 디지털 상호작용의 ‘통행료’를 받는 것이었습니다.

대한민국 정부가 내놓은 해답: 모바일 신분증

정부 발행 디지털 신분증

스마트폰에 발급되는 디지털 신분증으로, **실물 신분증(주민등록증, 운전면허증)과 동일한 법적 효력**을 가집니다.

2022 — 모바일 운전면허증

2024 — 모바일 주민등록증 (시범)

2025 — **모바일 주민등록증 전국 정식 발급**

목표

플라스틱 카드를 대체하고 온·오프라인에서 완벽하게 사용 가능한 포괄적 디지털 ID 인프라 구축.

> **"신원증명의 패러다임을 180도 바꾸는 혁신"**
> — 행정안전부

내 손안의 디지털 지갑: 데이터 주권은 사용자에게 돌아갑니다

핵심 기술

분산ID (DID) & 블록체인

신원 정보가 중앙 서버에 저장되지 않아 대량 데이터 유출을 방지합니다. 검증은 분산 원장을 통해 이루어집니다.

스마트폰 보안영역 저장

ID 데이터는 암호화되어 사용자의 기기 내 보안 칩(TEE/eSE)에 안전하게 보관됩니다.

선택적 정보 공개

사용자가 어떤 정보를 누구에게 공유할지 완벽하게 제어합니다.

시각적 설명

자기주권 신원증명 (SSI) 원리

이 변화는 한국만의 이야기가 아닙니다: 유럽은 eIDAS 2.0으로 앞서가고 있습니다

eIDAS 2.0이란?

EU의 차세대 디지털 신원 전략으로, **EU 디지털 신원 지갑 (EU Digital Identity Wallet)**을 중심으로 합니다.

2026년까지 모든 27개 EU 회원국은 시민에게 **최소 하나 이상의 공인 디지털 지갑을 제공**해야 하는 **법적 의무**를 가집니다.

EU 전역에 걸쳐 **단일하고 상호 운용 가능한 신뢰 프레임워크**를 구축하여, 국경을 넘나드는 원활하고 안전한 서비스를 가능하게 합니다.

하나의 지갑, EU 전체의 신뢰: eIDAS 2.0이 재정의하는 디지털 주권

사용자 중심 및 자기주권 신원 (User-Centric & SSI)

사용자는 지갑에 저장된 자신의 신원 데이터에 대한 완전한 통제권을 가집니다.

데이터 최소화 및 선택적 공개

법적으로 필요한 최소한의 정보만 공유하도록 설계되었습니다.
(예: 생년월일 대신 '성인 여부'만 증명)

공공 주도, 민간 참여

신뢰 프레임워크는 공공이 수립하며, 인증된 민간 기업은 그 안에서 지갑을 개발하거나 서비스를 제공할 수 있습니다.

빅테크 플랫폼 의무 수용

대형 온라인 플랫폼(Google, Facebook 등)은 로그인을 위해 EU 디지털 신원 지갑을 의무적으로 수용해야 합니다.

세 가지 시스템, 하나의 질문: 누가 데이터의 주인인가?

Feature	민간 CI/DI (Private CI/DI)	대한민국 모바일 신분증 (Korea Mobile ID)	EU eIDAS 2.0
주체 (Sovereign)	민간 기업 (Private Co.) 🔴	대한민국 정부 (Government) 🟢	EU 및 회원국 정부 (EU & Member States) 🟢
데이터 저장소 (Data Storage)	중앙 서버 (Central Server) 🔴	사용자 스마트폰 (User's Smartphone) 🟢	사용자 지갑 (User's Wallet) 🟢
정보 공개 (Info Disclosure)	전체 식별자 전송 (Full Identifier Transfer) 🔴	선택적 공개 (Selective Disclosure) 🟢	데이터 최소화 법제화 (Minimization by Law) 🟢
사용자 통제권 (User Control)	없음 (None) 🔴	완전 통제 (Full Control) 🟢	완전 통제 (Full Control) 🟢
법적 효력 (Legal Effect)	사설 인증 (Private Authentication)	실물 신분증과 동일 (Same as Physical ID) 🟢	EU 전역 상호인증 (EU-wide Mutual Recognition)

정부는 신뢰의 앵커가 되고, 민간은 혁신의 파트너가 됩니다

정부의 새로운 역할: 신뢰의 앵커

- 신원 발급의 유일한 주체
- 신뢰 프레임워크와 기술 표준 수립
- 국민의 데이터 주권 보장

민간의 새로운 기회: 혁신의 파트너

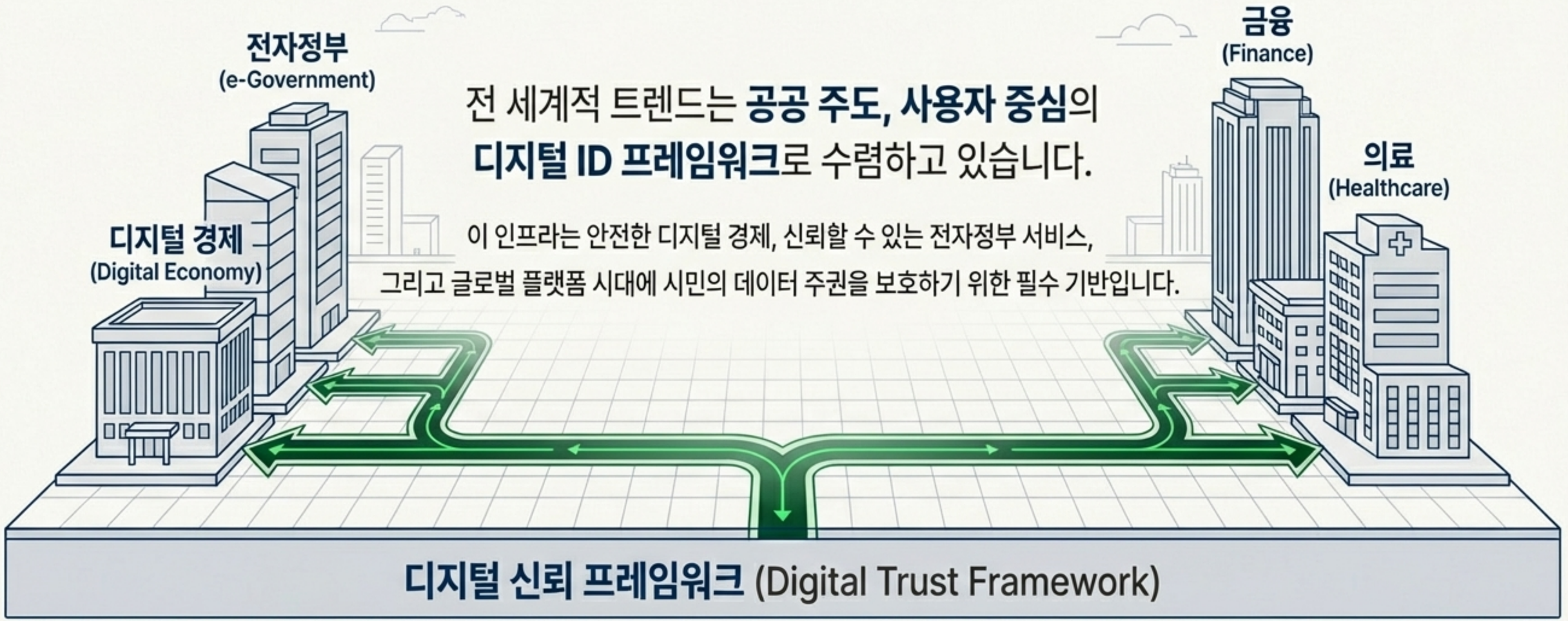
- **'통행료 징수원'**에서 **'혁신 파트너'**로': 민간 기업 (네이버, 카카오, 은행 등)은 신원 발급자가 아닌, **정부가 승인한 지갑 운영자** 및 서비스 제공자가 됩니다.
- 핵심 신원 데이터를 관리할 책임 없이, 안전한 공공 인프라 위에서 혁신적인 서비스를 구축할 수 있습니다.
- 데이터 독점이 아닌 가치 창조에 집중하는 건강한 생태계가 조성됩니다.

2025년 전국민 발급: 모바일 주민등록증이 바꿀 대한민국의 디지털 일상

2024년 말까지 **400만 건 발급** 달성, 2025년 전국민 확대

- **온·오프라인 통합** 하나의 신분증으로 정부 서비스, 은행, 공항, 투표, 상점 내 연령 확인까지.
- **민간 인증 대체** 웹사이트와 앱에서 비용과 보안 위험이 높은 PASS 인증 대신 모바일 신분증 API 채택 가속화.
- **행정 효율화** 장기적으로 플라스틱 신분증 제작 및 관리 비용 절감.

디지털 신원은 21세기의 사회 기본 인프라입니다



전 세계적 트렌드는 **공공 주도, 사용자 중심**의 **디지털 ID 프레임워크**로 수렴하고 있습니다.

이 인프라는 안전한 디지털 경제, 신뢰할 수 있는 전자정부 서비스, 그리고 글로벌 플랫폼 시대에 시민의 데이터 주권을 보호하기 위한 필수 기반입니다.

국민의 식별자를 민간이 소유할 이유는 더 이상 없습니다.

이제, 시스템을 다시 설계할 시간입니다.