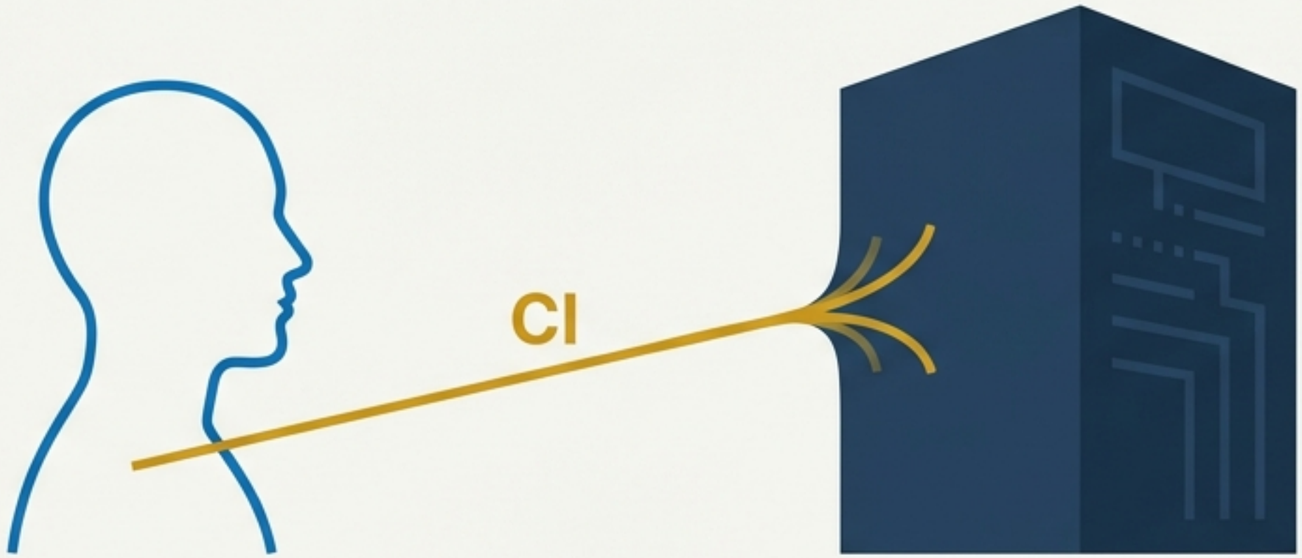
A Citizen’s Identity Should Not Be a Private Asset.



“Why did my national identifier become a core asset for a private company?”

“This isn’t a security industry. It’s a tollbooth industry created by regulation.”

For decades, South Korea’s online identity system was built on a private model. This deck examines that legacy, the public-led revolution replacing it, and its alignment with a new global standard.

The Legacy Model: When a ‘Replacement’ Becomes a Permanent Digital Shadow.

South Korea’s CI/DI System

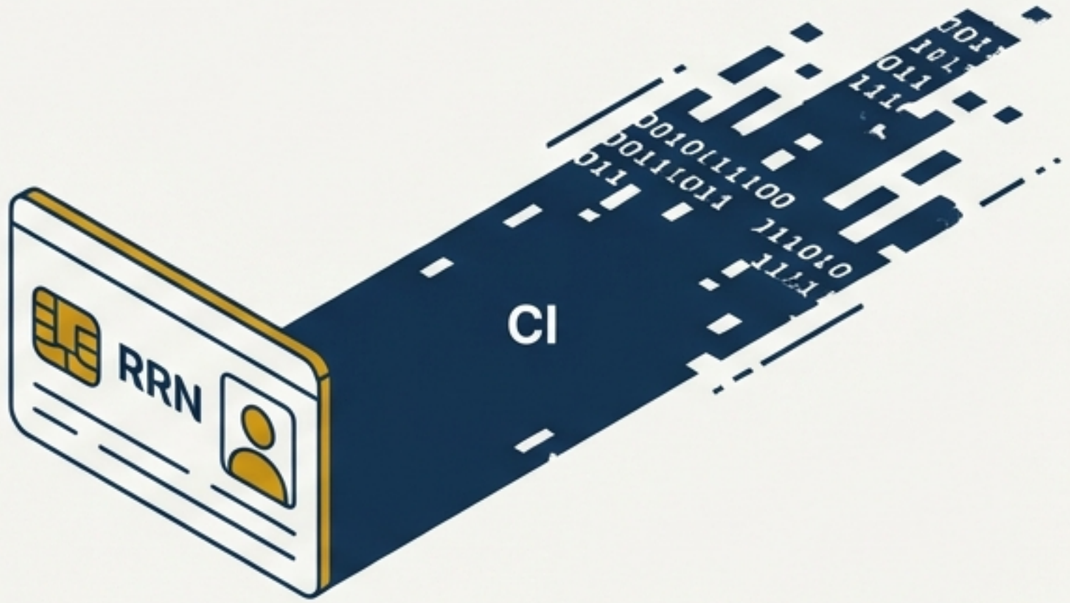
The long-standing method for online identity verification, created to stop the rampant collection of national **Resident Registration Numbers** (RRNs).

CI (Connection Information)

An 88-byte encrypted value. One permanent, unchangeable CI is issued per person for life, designed to link a person’s activities across different online services.

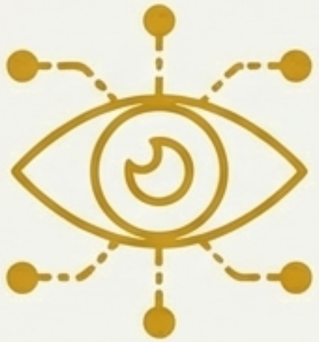
DI (Duplication Information)

A 64-byte value issued per person, per website, to prevent duplicate accounts.



The CI is 1:1 mapped to the RRN, making it an “Online Resident Registration Number.” It solved one problem by creating another with the same fundamental privacy risks.

Four Structural Flaws of the Private 'Tollbooth' Model.



Privacy Failure

The CI acts as a universal 'super-cookie,' allowing companies to track and link a user's online activities across different services, often without explicit, ongoing consent.

No User Control

Citizens have no power to change or revoke their CI, even after a data breach. The identifier is permanent, controlled by the issuing private institutions (telecom companies, credit agencies).

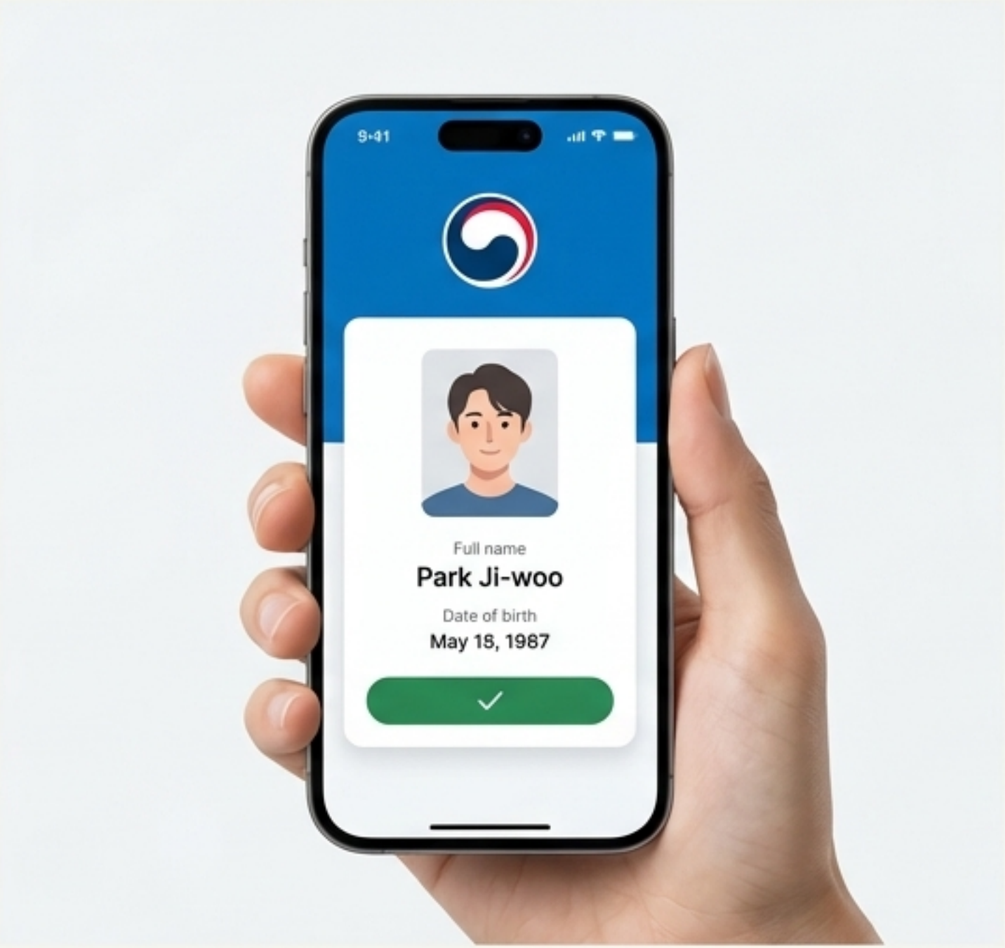
A Closed, National System

The entire system is dependent on the Korean RRN, making it exclusionary for foreigners and incompatible with global standards.

Centralized Risk

The process relies on private companies' central databases to verify identity, creating high-value targets for hacking and potential for mass data leakage.

The Public-Led Answer: South Korea's Official Mobile ID



A Government-Issued Digital ID

- **What it is:** A government-issued digital ID stored securely on a smartphone.
- **Legal Power:** It has the **exact same legal validity** as its physical counterpart (Driver's License, Resident Registration Card).
- **The Goal:** To replace plastic ID cards and create a unified, secure infrastructure for all online and offline identification needs.
- **Rollout:** Phased introduction since 2021, with the Mobile Resident Registration Card set for nationwide launch in 2025.

Shifting Power to the User with Self-Sovereign Identity (SSI) Principles

On-Device Security

ID data is encrypted and stored in the smartphone's secure element (TEE or eSE), not on a central server.

Decentralized Verification

Uses blockchain-based Distributed ID (DID) technology to verify authenticity without a central database lookup, preventing mass data leaks.

Selective Disclosure Example

For age verification, the app shares only a 'Yes/No' for adulthood, not the user's full name, address, or birthdate.

A Global Convergence: The EU Mandates a New Standard with eIDAS 2.0.

eIDAS 2.0

The EU's next-generation digital identity framework, centered on the **EU Digital Identity Wallet (EUDIW)**, which must be offered to every EU citizen by 2026.

Key Mandates

Interoperability: One wallet, valid across all 27 EU member states for public and private services.

User-Centricity: Legally enshrines principles of data minimization and user control (SSI).

Market Integration: Mandates that Very Large Online Platforms (e.g., Google, Meta) must accept the EUDIW for login, breaking dependency on private identity systems.

Three Competing Models for Digital Identity

The Legacy Private Model

South Korea: Private CI/DI
Inter SemiBold

Privately operated system based on a permanent, centralized identifier.

The National Public Model

South Korea: Mobile ID
Inter SemiBold

Government-issued digital version of a legal ID, emphasizing on-device storage and user control.

The Supra-National Public Framework

European Union: eIDAS 2.0 Wallet
Inter SemiBold

A cross-border trust framework mandating interoperable, user-controlled digital wallets for all citizens.

Comparison: Who Governs the System?

	 **The Legacy Private Model** South Korea: Private CI/DI	 **The National Public Model** South Korea: Mobile ID	 **The Supra-National Public Framework** European Union: eIDAS 2.0 Wallet
Primary Actor & Governance	**Private Sector Led.** Telecom and financial institutions operate the system for profit, under government regulation.	**Government Led.** The state is the sole issuer of identity. Private firms (e.g., Naver, Kakao) can act as certified 'wallet operators' but do not create the identity.	**Public Trust Framework.** EU regulations set the rules. Member states must provide at least one official wallet, but certified private companies can also offer wallets.
Legal Status & Authority	**De Facto Authentication.** Not a legal ID. Serves as a means of identity verification based on private contracts.	**Legally Equivalent to Physical ID.** Backed by national laws (e.g., Resident Registration Act). Legally binding for all public and private transactions.	**Legally Binding across the EU.** Mandated by EU regulation. Guarantees cross-border recognition and legal validity.

Comparison: Technology and Privacy by Design.

	 **The Legacy Private Model** South Korea: Private CI/DI	 **The National Public Model** South Korea: Mobile ID	 **The Supra-National Public Framework** European Union: eIDAS 2.0 Wallet
Core Technology	**Centralized Database Lookup.** Relies on matching user data against a central store held by a private institution.	**On-Device Storage & DIDs.** Uses smartphone Secure Element and blockchain (DID) for decentralized verification.	**Digital Wallet & Verifiable Credentials (VCs).** Utilizes advanced cryptographic methods like Zero-Knowledge Proofs (ZKP) for maximum privacy.
Privacy Approach	**High Privacy Risk.** The permanent CI enables cross-site user tracking. User data is repeatedly provided to the central institution for every verification.	**Privacy-Enhancing.** No central PII server. User controls data sharing via selective disclosure on the device.	**Privacy by Design (Legally Mandated).** User sovereignty is the core principle. Data minimization and selective disclosure are required by law. User consent is paramount.

The Inevitable Conflict: Public Infrastructure Replaces the Private Tollbooth

Functional Replacement

The Mobile ID can perform every function of CI/DI (e.g., website login, age verification, KYC for finance) but with higher legal authority and security.

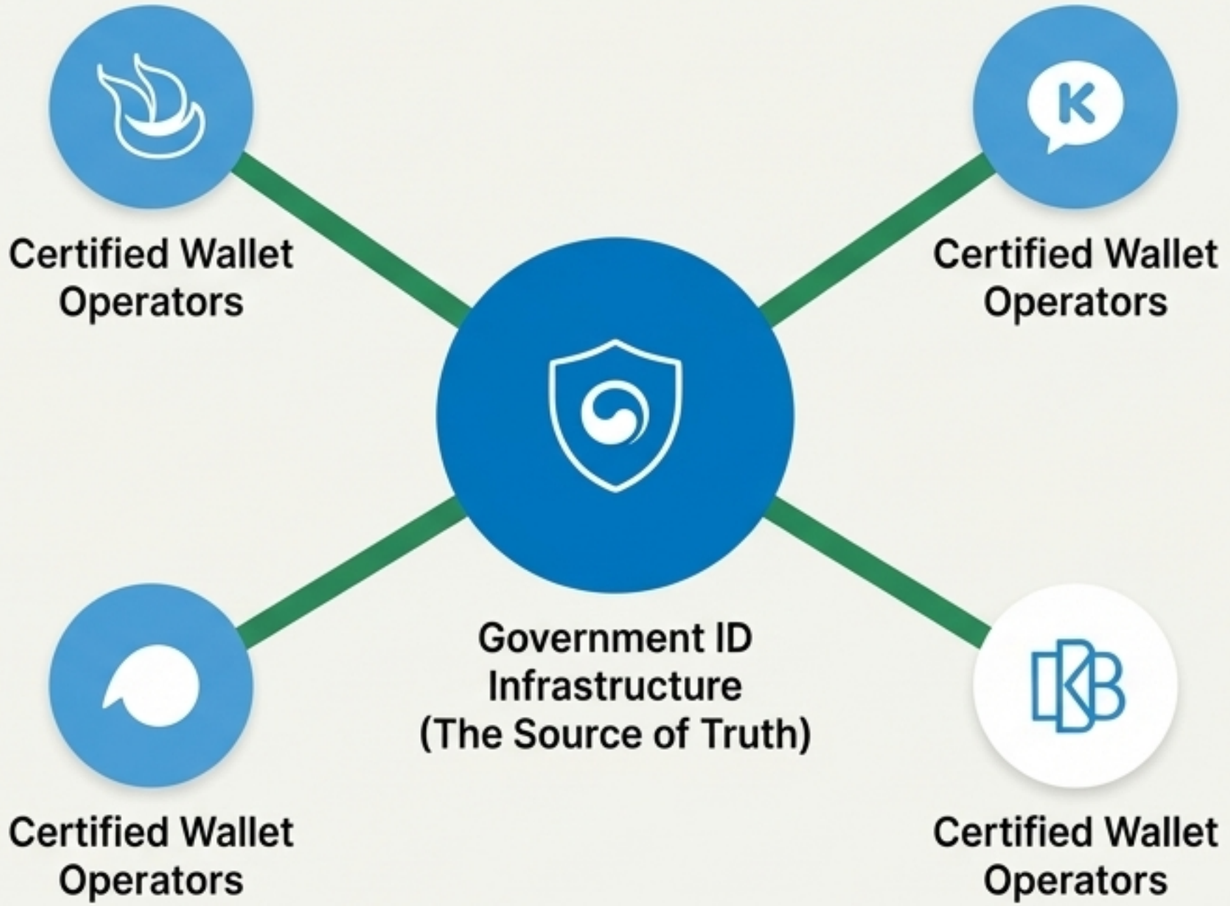
Threat to Incumbents

The rise of a free, public ID infrastructure directly threatens the fee-based business model of the telecom companies and other institutions that profited from the CI/DI “tollbooth”.

Data Control Shift

For internet companies, the shift from receiving a permanent CI to dealing with privacy-preserving, selective disclosure from a Mobile ID means a loss of the ability to easily link and track user data.

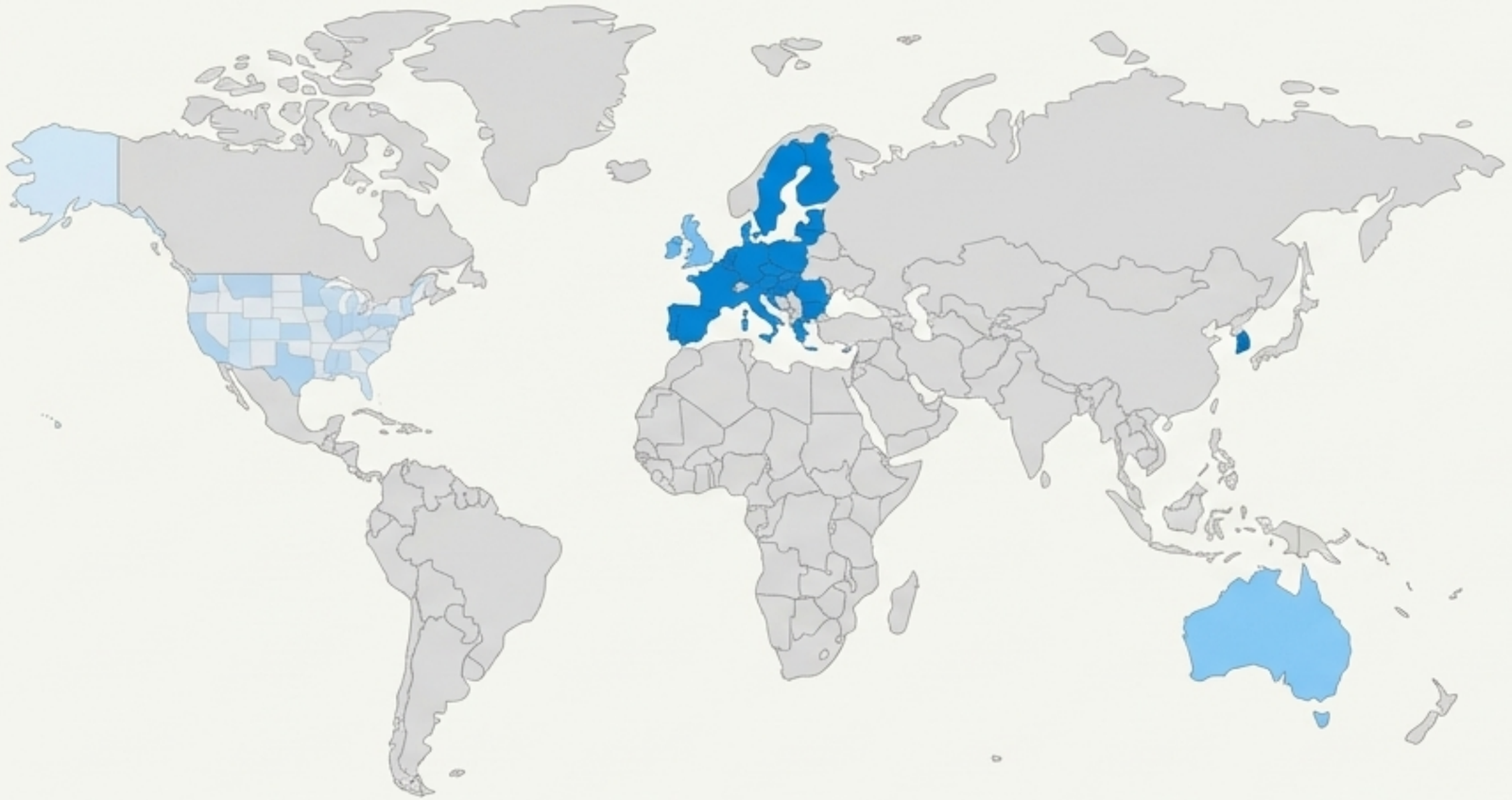
A Path to Coexistence: Integrating Private Platforms into the Public Ecosystem.



The Korean government is not building its own app exclusively. It is certifying major private platforms (Naver, Kakao, banks) to host the Mobile ID within their existing, widely-used applications.

- ✅ **Rapid Adoption:** Leverages the massive user bases of existing tech platforms to accelerate rollout.
- ✅ **Industry Soft Landing:** Provides a new, valuable role for former incumbents, transforming them from ‘tollbooth operators’ into ‘trusted infrastructure partners’.
- ✅ **User Convenience:** Allows citizens to use the ID service within the apps they already use daily.

The Global Consensus: Digital Identity is Sovereign Infrastructure



Key Global Trends

Public Leadership is the Norm

Governments worldwide are recognizing that a trusted digital identity is fundamental public infrastructure, like roads or currency.

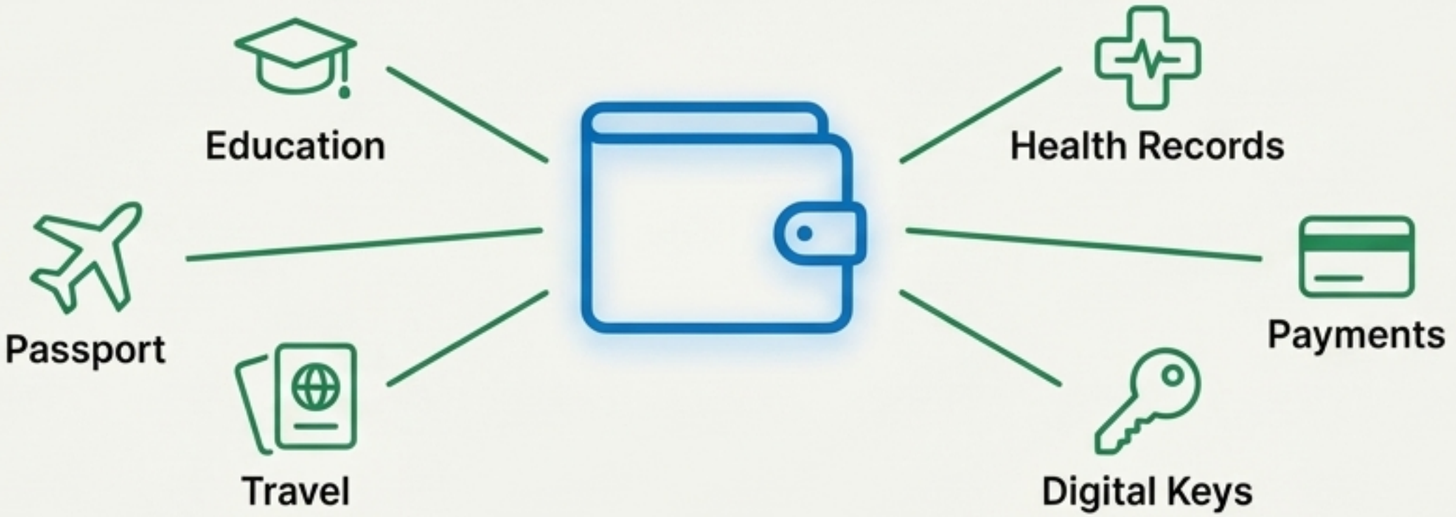
From Fragmentation to Frameworks

Countries like Australia and the UK are moving away from purely private solutions to establish national "Trust Frameworks," inspired by models like eIDAS.

The Goal of Digital Sovereignty

The core driver is the need for nations to control their own identity infrastructure, ensuring it serves the public interest rather than the commercial interests of Big Tech or other private entities.

Beyond Identification: The Wallet as a Hub for Digital Life.



Future Vision in Europe (eIDAS 2.0)

- The EU wallet is explicitly designed to hold more than just identity.
- Future use cases include: University Diplomas, Medical Prescriptions, Digital Driver's Licenses, and Payment Credentials.
- The goal is a single, secure wallet for all of a citizen's official credentials.

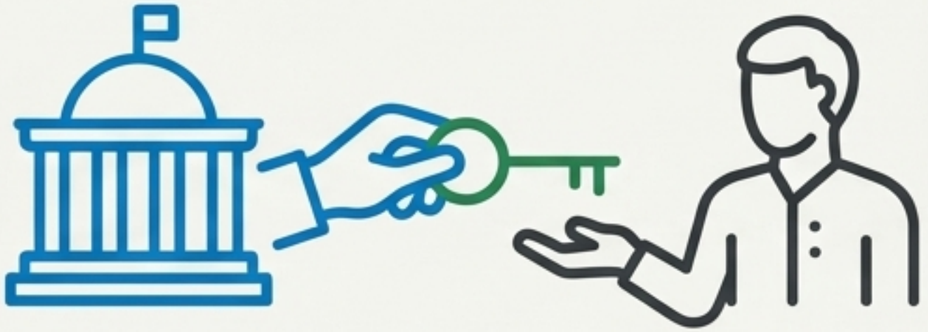
Future Vision in South Korea (Mobile ID)

- The immediate goal is full replacement of plastic IDs and deep integration into online services, replacing CI/DI as the standard.
- Long-term plans include expanding to a Mobile Foreigner Registration Card to enhance digital inclusion.
- The government aims to foster an ecosystem where the Mobile ID is the default method for all on/offline identity transactions.

The Three Models at a Glance: A Strategic Summary

Dimension	Private CI/DI (The Past)	SK Mobile ID (The Present)	EU eIDAS 2.0 (The Future)
Governance	Private Sector Led (Telcos)	**Government** Issued & Controlled	**Public Trust Framework** (EU-wide)
User Control	None (**Permanent Identifier**)	**High** (On-device, Selective Disclosure)	**Absolute** (Legally Mandated SSI)
Privacy Model	**Surveillance by Design**	**Privacy-Enhancing**	**Privacy by Design**
Private Role	**Tollbooth Operator**	**Certified Wallet Partner**	**Certified Ecosystem Participant**
Legal Force	**Contractual Verification**	Equal to Physical ID	**Legally Binding Across Borders**
Trajectory	Obsolete / Declining	**National Standard** / **Expanding**	**Global Benchmark** / **In Rollout**

The Future of Identity is Public, Portable, and Private.



The era of treating citizen identity as a private, commercial asset, as exemplified by the CI/DI model, is over.

The new global standard, demonstrated by both South Korea's Mobile ID and the EU's eIDAS 2.0, is a public-private partnership built on a foundation of public trust.

In this new model, the government's role is to guarantee the authenticity and security of identity, while technology empowers the citizen with ultimate control.

The fundamental question has been answered. A citizen’s identity belongs to the citizen—and the infrastructure of the future will be built to enforce that right.