Why do 850 million people lack official identity — and why does KYC cost banks $60 billion?

The identity problem has two sides:

Side 1 — Exclusion:

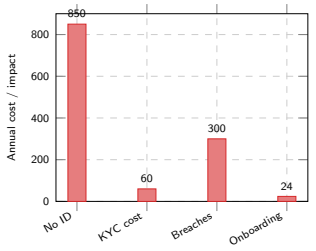
- 850 million people globally lack official identity documents (World Bank)
- Without ID: no bank account, no SIM card, no government services
- Refugees, stateless persons, rural populations most affected
- Birth registration rates below 50% in parts of Sub-Saharan Africa

Side 2 — Cost and friction:

- Banks spend $60 billion/year on KYC (Know Your Customer) compliance
- Average KYC onboarding takes 24 days per customer
- Each customer verified independently by every institution
- Data breaches expose millions of identity records annually

The paradox:
Your identity is controlled by governments (passports) and corporations (logins). You cannot take it with you, and they lose it in data breaches.

Key insight: Identity today is institutional — you prove who you are by asking someone else to vouch for you.



Units: No ID = millions of people (Source: World Bank Findex 2024); KYC cost = $ billions (Source: LexisNexis, Fenergo); Breaches = millions of records/year (Source: IBM Cost of a Data Breach 2024); Onboarding = days.

Every institution builds its own identity silo. You are verified from scratch every time you open a bank account, sign a lease, or start a job.

Identity is the foundation of financial access — 850 million people are excluded because they cannot prove who they are to institutions.

Imagine proving you are over 18 without showing your birthday, name, or address

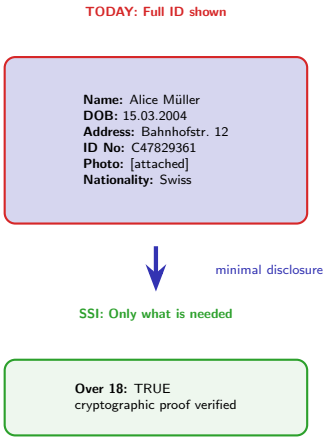
The scenario:
You walk into a bar. The bouncer asks for ID. Today, you hand over your passport or driving licence — revealing your full name, date of birth, address, photo, and ID number.

With self-sovereign identity:
You hold your phone up. The bouncer's scanner receives a single piece of information: "over 18 = true." That is all. Cryptographically proven, government-issued, instantly verified.

What was NOT revealed:

- Your name
- Your exact date of birth
- Your address
- Your photo
- Your ID number

This is called selective disclosure:
You prove exactly what is needed — nothing more. The verifier gets a cryptographic proof, not your personal data.



The shift: From "show me everything" to "prove only what I need."

Selective disclosure means you can prove claims about yourself without revealing the underlying data — privacy by design, not privacy by policy.

How does self-sovereign identity work — issuers, holders, and verifiers?

Definition: Self-Sovereign Identity (SSI)

A model where individuals hold their own digital credentials in a personal wallet, choosing what to share with whom. Credentials are cryptographically signed by issuers and verified without contacting the issuer.

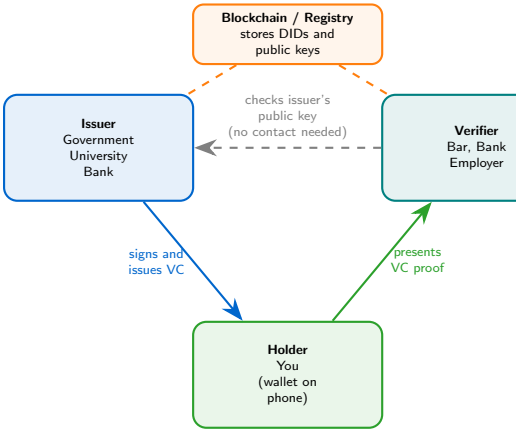
The three roles:

1. **Issuer:** organisation that creates and signs a credential (e.g., university issues a diploma, government issues age proof)
2. **Holder:** you — stores credentials in a digital wallet on your phone
3. **Verifier:** the party that checks the credential (e.g., bar, bank, employer)

Two key standards:

- **Verifiable Credentials (VCs):** tamper-proof digital certificates
- **Decentralised Identifiers (DIDs):** globally unique IDs controlled by the holder, not a central authority

Key insight: The verifier checks the credential's cryptographic signature — it never needs to contact the issuer, unlike today's centralised systems.



The trust triangle separates issuing from verifying — the holder controls what to share, and the verifier never needs to call the issuer.

How will eIDAS 2.0 give 450 million Europeans a digital identity wallet?

EU eIDAS 2.0 regulation:

- Requires every EU member state to offer a Digital Identity Wallet
- Target: available to all 450 million EU citizens
- Wallet stores government-issued credentials (ID, driving licence, diploma)
- Cross-border: French wallet works in German bank, Italian hotel

What the wallet will hold:

- National ID / passport equivalent
- Driving licence
- University diplomas and professional certificates
- Health insurance cards
- Bank account proofs
- Age verification for online services

Key design principles:

- User controls what to share (selective disclosure)
- Government cannot see when or where you present credentials
- Private companies must accept the wallet (mandatory acceptance)
- Free for citizens

Feature	eIDAS 2.0
Population	450 million
Launch target	2026–2027
Wallet cost	Free for citizens
Cross-border	Yes (all 27 member states)
Credentials	ID, licence, diploma, health
Selective disclosure	Yes
Mandatory acceptance	Yes (large platforms)
Technology	Not prescribed (blockchain optional)
Privacy	Government cannot track presentations

Pilot programmes:

- POTENTIAL (Germany, France, 6 others)
- NOBID (Nordic/Baltic payments)
- EU Digital Identity Wallet Toolbox
- 4 large-scale pilots running 2023–2025

How does SSI change opening a bank account — from 24 days to 24 seconds?

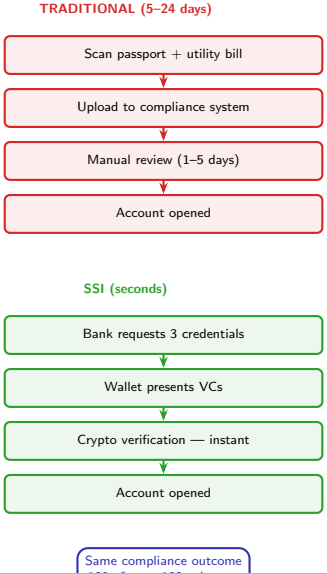
Today — traditional KYC:

1. Visit branch or upload documents online
2. Scan passport or ID card
3. Provide utility bill for address proof
4. Bank sends documents to compliance team
5. Manual review: 1–5 business days
6. Additional checks for politically exposed persons
7. Account opened after 5–24 days
8. Cost per customer: $30–$300

With SSI:

1. Bank requests: "proof of identity, proof of address, proof of tax residency"
2. Your wallet presents three Verifiable Credentials
3. Bank verifies cryptographic signatures instantly
4. Account opened in seconds
5. Cost: near zero (no manual review)

Key insight: SSI does not eliminate KYC — it makes it instant by reusing credentials already verified by trusted issuers.



What can go wrong with self-sovereign identity — from lost phones to trust paradoxes?

Key management — the smartphone problem:

- Lose phone = lose access to credentials?
- Recovery trade-off: too easy invites theft, too hard locks you out

The issuer trust problem:

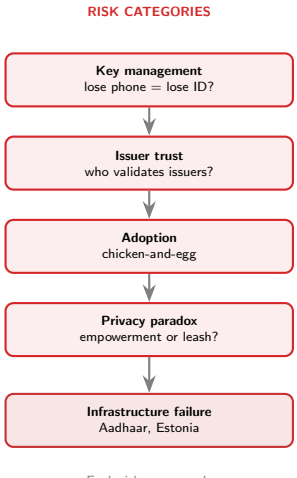
- SSI credentials are only as trustworthy as the issuer
- A diploma from a fake university is still cryptographically valid
- Who decides which issuers are trusted? (trust frameworks needed)

The adoption chicken-and-egg:

- Holders will not adopt wallets without verifiers accepting them
- Verifiers will not integrate without holders using it
- Regulation (eIDAS 2.0) attempts to break this deadlock

Real-world failures:

- **India Aadhaar (2018):** The world's largest biometric ID system (1.4B records) suffered multiple data breaches. Full identity records could be purchased for the equivalent of $8. Centralised identity databases are high-value targets.
- **Estonia (2017):** A cryptographic flaw in 750,000 government-issued digital ID cards allowed private keys to be computed from public keys. Cards had to be revoked and reissued — even sophisticated digital ID systems can fail at the infrastructure level.



SSI shifts the trust problem but does not eliminate it — even the most advanced digital ID systems (Aadhaar, Estonia) have suffered critical failures.

Where is self-sovereign identity being built — from EU regulations to crypto protocols?

Government-led initiatives:

- **EU eIDAS 2.0:** largest programme, 450M citizens, 2026–2027
- **India Aadhaar:** 1.3B biometric IDs (centralised, not SSI)
- **World Bank ID4D:** digital identity for developing nations
- **Canada Pan-Canadian Trust Framework:** SSI governance

Technology platforms:

- **Microsoft ION:** decentralised identity on Bitcoin (Layer 2)
- **Hyperledger Indy:** open-source SSI blockchain
- **Cheqd:** payment rails for verifiable credentials
- **Spruce / SpruceID:** Ethereum-based identity
- **Polygon ID: zero-knowledge proofs** — a cryptographic method that lets you prove a statement is true ("I am over 18") without revealing the underlying data (your birth date). The verifier learns nothing except that the statement is true.

W3C standards (W3C = World Wide Web Consortium, the international standards body for web technologies)**:**

- Verifiable Credentials (VCs) — W3C standard since 2019
- Decentralised Identifiers (DIDs) — W3C standard since 2022
- These ensure wallets from different providers can interoperate.

Project	Type	Scale
eIDAS 2.0	Govt	450M citizens
Aadhaar	Govt	1.3B (central)
ID4D	Intl	1B+ target
MS ION	Corp	Bitcoin L2
Hyperledger	OSS	Enterprise
Polygon ID	Crypto	ZK proofs

Two competing visions:

- **Government-led:** eIDAS 2.0 — regulated, centralised issuance, interoperable wallets
- **Crypto-native:** Polygon ID, ION — permissionless, zero-knowledge, decentralised

Both approaches use the same W3C standards (VCs, DIDs), so they can potentially interoperate.

Does self-sovereign identity empower individuals or enable new forms of surveillance?

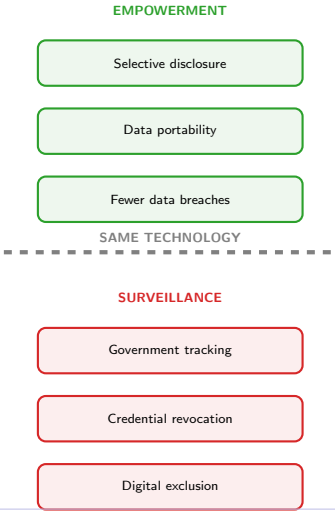
The empowerment case:

- **Data minimisation:** share only what is needed (selective disclosure)
- **Portability:** take your credentials to any service provider
- **Inclusion:** digital identity for refugees and stateless persons
- **Reduced data breaches:** verifiers do not need to store your data
- **User consent:** you decide when to share, with whom

The surveillance case:

- Government controls the wallet app — can it track usage?
- "Mandatory acceptance" means services *require* digital ID
- Credential revocation becomes a tool of control
- Digital exclusion: those without smartphones are left out
- Correlation attacks: linking credentials across services reveals behaviour patterns

Key insight: The same technology that enables "prove your age without your name" also enables "revoke someone's digital identity remotely." Design choices determine which outcome dominates.



SSI is a tool — whether it serves privacy or surveillance depends entirely on governance, regulation, and implementation choices.

So what? One sentence to remember about self-sovereign identity

SSI flips identity: you carry credentials

instead of asking institutions to vouch for you —

but adoption requires all three parties to participate.

What SSI solves	What SSI does not solve	What determines outcome
Data minimisation	Key management risk	Governance framework
Instant KYC	Issuer trustworthiness	Open vs closed wallets
Cross-border portability	Chicken-and-egg adoption	Privacy regulation
Fewer data breaches	Digital divide	Interoperability standards

SSI is the most important infrastructure shift since the internet — it changes who controls identity, but the outcome depends on who builds and governs the wallets.

Your turn: would you trust a blockchain-based digital identity issued by your government?

Discussion Question

Your government announces a digital identity wallet. It will hold your passport, driving licence, and health card. It uses selective disclosure — you can prove your age without revealing your name.

Would you trust it? What are the risks?

- Can the government track when and where you use your credentials?
- What happens if the government revokes your digital identity?
- Should the wallet be open-source so anyone can audit it?
- Should private companies (Apple, Google) be allowed to build competing wallets?

Further Reading

- EU eIDAS 2.0 regulation: `digital-strategy.ec.europa.eu/en/policies/eidas-regulation`
- Allen (2016), "The Path to Self-Sovereign Identity" (foundational essay)
- W3C Verifiable Credentials: `w3.org/TR/vc-data-model/`

Reflection