Self-Sovereign Identity: You Own Your Data

Module 3: The Trust Problem — Companion Lecture

Prof. Dr. Joerg Osterrieder

Digital Finance — BSc Course

Companion lecture — explores why digital identity is broken and how Self-Sovereign Identity (SSI) aims to fix it.

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:

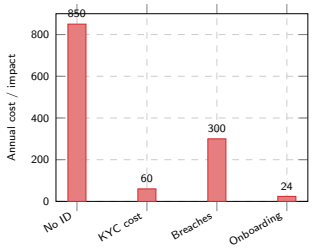
- 850 million people globally lack official identity documents (World Bank)
- Without ID: no bank account, no SIM card, no government services
- Refugees, stateless persons, rural populations most affected
- Birth registration rates below 50% in parts of Sub-Saharan Africa

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

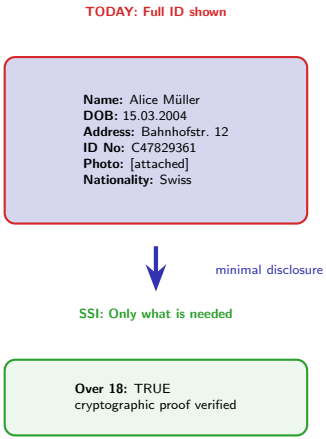
The scenario:
You walk into a bar. The bouncer asks for ID. Today, you hand over your passport or driving licence — revealing your full name, date of birth, address, photo, and ID number.

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.

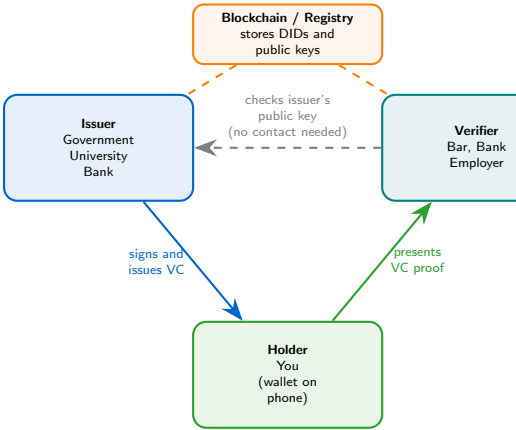
The three roles:

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?

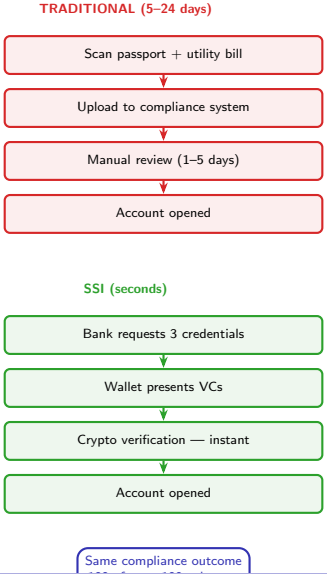
Today — traditional KYC:

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:

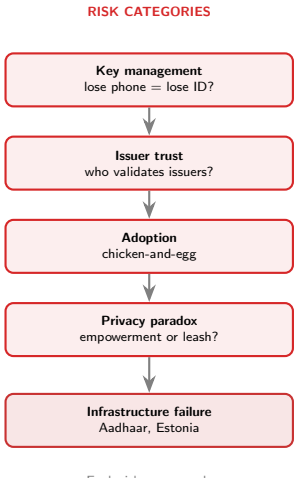
- SSI credentials are only as trustworthy as the issuer
- A diploma from a fake university is still cryptographically valid
- Who decides which issuers are trusted? (trust frameworks needed)

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?

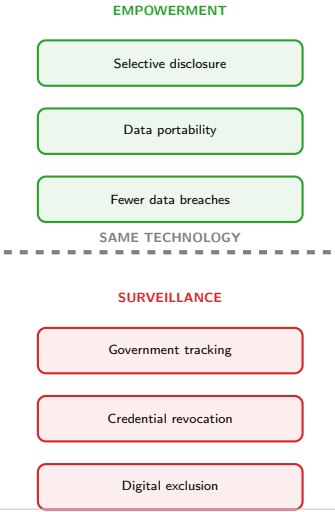
The empowerment case:

- **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?

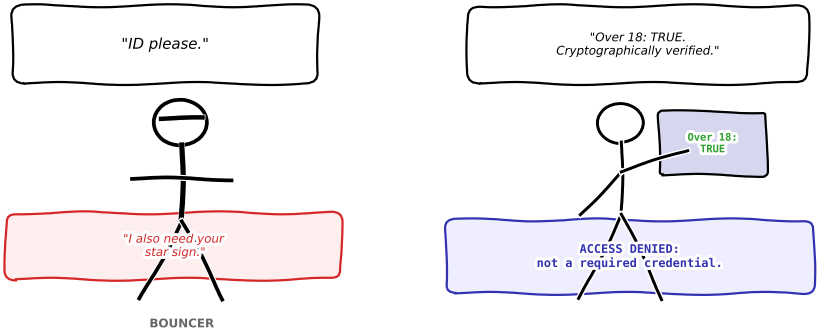
- Can the government track when and where you use your credentials?
- What happens if the government revokes your digital identity?
- Should the wallet be open-source so anyone can audit it?
- Should private companies (Apple, Google) be allowed to build competing wallets?

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

Self-Sovereign Identity



Self-sovereign identity: you decide what to share.

The core idea: you share only what is needed — nothing more.

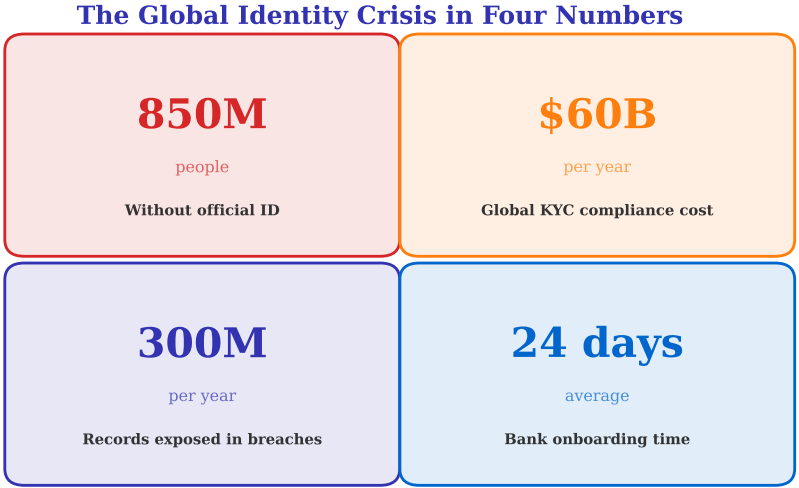
Learning Objectives

After completing this lecture, you will be able to:

1. **Explain** why centralized identity systems create systemic risk for individuals and institutions [Understand]
2. **Describe** the SSI trust triangle (Issuer, Holder, Verifier) and how Verifiable Credentials (VCs) work [Understand]
3. **Apply** Zero-Knowledge Proofs (ZKPs) to real-world identity scenarios [Apply]
4. **Compare** traditional Know Your Customer (KYC) with SSI-based onboarding [Analyze]
5. **Evaluate** the privacy–surveillance trade-off in government-led digital identity [Evaluate]

Bloom's levels covered: Understand, Apply, Analyze, Evaluate

Objectives follow Bloom's taxonomy: Understand → Apply → Analyze → Evaluate.



What you see: four statistics that frame the scale of the problem — 850 million people lack official ID, compliance costs $60 billion per year, breaches

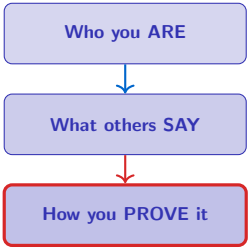
What Does "Identity" Even Mean?

Three layers of identity:

1. **Who you are** — biometrics, personality, memories
2. **What others say about you** — credentials, diplomas, credit scores
3. **How you prove it** — documents, passwords, tokens

The problem:

Today, layer 3 is controlled by **others** — governments issue passports, banks verify addresses, universities grant diplomas. You carry the credentials but never truly *own* them.



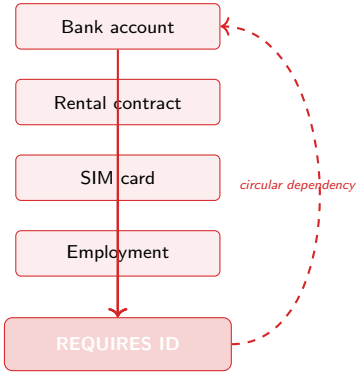
Key insight: your identity is a relationship between these three layers — SSI aims to give you control over layer 3.

Meet Amira: Identity Without Documents

Amira, 28, Syrian refugee in Germany

- Fled Syria in 2015 with no documents
- Has a degree in computer science — no proof
- Speaks three languages — cannot certify any
- Cannot open a bank account, rent an apartment, or get a SIM card

The paradox: To get identity documents, you need identity documents. 850 million people worldwide face some version of this trap.



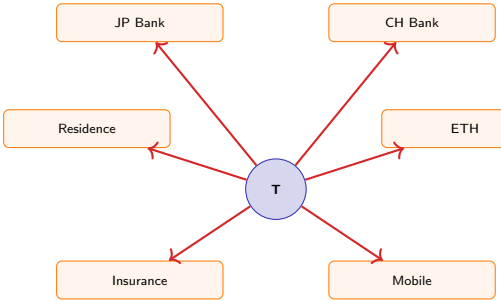
Amira's story is fictional but representative — the World Bank estimates 850 million people lack official ID (ID4D dataset, 2023).

Meet Tomoko: Identity Fragmentation

Tomoko, 22, Japanese student at ETH Zurich

- Verified her identity for her Japanese bank
- Re-verified for her Swiss residence permit
- Re-verified again for her Swiss bank account
- Re-verified for her ETH student account
- Re-verified for her health insurance
- Re-verified for her mobile phone contract

Six times the same information, submitted to six different organizations. Each stores a copy. Each is a breach target.



6 copies of her data

Every copy is a liability — Tomoko has no control over how these organizations store, share, or lose her data.

Meet Diego: KYC Exhaustion

Diego, 35, Brazilian freelance developer

- Works for clients in 4 countries
- Completed **7 separate KYC processes** this year
- Each took 3–4 weeks of document uploads, video calls, and waiting
- Total time lost: **5+ months** of part-time effort
- One platform rejected his ID because Brazil uses a different date format

The cost: Diego is not unbanked — he is *over-verified*. The system trusts none of its own previous checks.

The global KYC compliance cost is estimated at $60 billion annually (Thomson Reuters, 2023) — SSI would let Diego verify once and reuse.

How many times have you shown your ID this year?

A) 1–3 times

B) 4–10 times

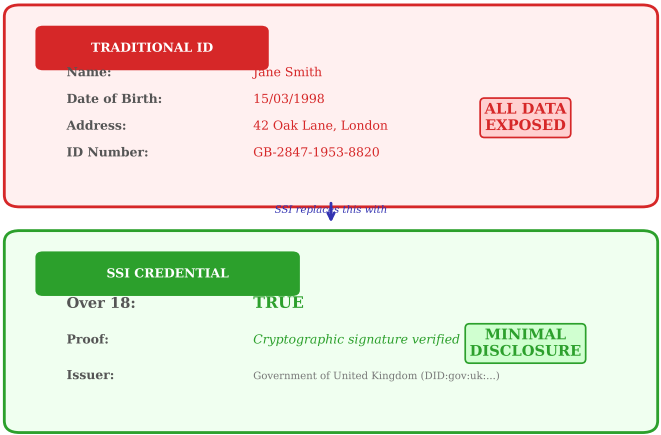
C) 10–20 times

D) I lost count

Each time, you handed over more data than necessary.

Most students underestimate — include bank logins, age verification, travel, uni registration, gym membership, and more.

What You Share Today vs What You Need To



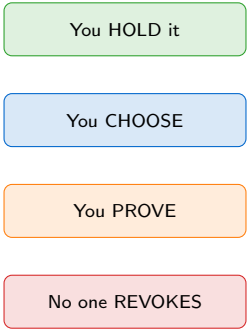
What you see: a traditional ID exposes all data (name, DOB, address, ID number) even when the verifier only needs to know your age.

The Core Idea: Self-Sovereign Identity

Self-Sovereign Identity (SSI) means:

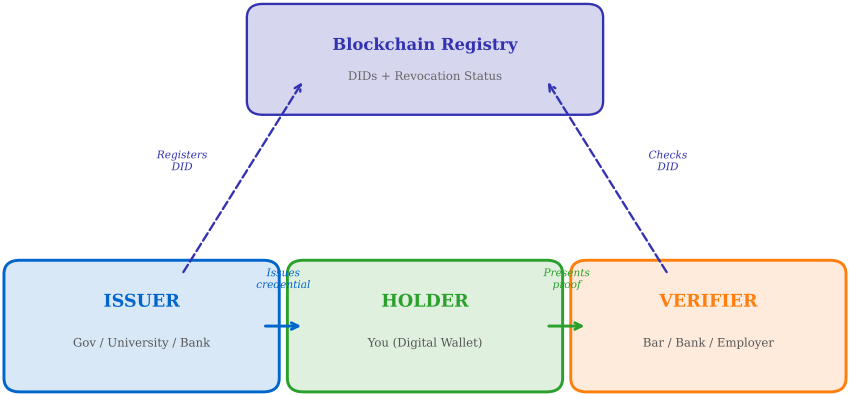
1. You **hold** your own credentials (in a digital wallet)
2. You **choose** what to share and with whom
3. You **prove** claims without revealing underlying data
4. No central authority can revoke your identity unilaterally

Analogy: Your physical wallet. You carry your cards. You decide which card to show. The bartender does not call the government to check.



The term "self-sovereign" was coined by Christopher Allen in 2016 — 10 principles including existence, control, access, transparency, persistence.

The SSI Trust Triangle



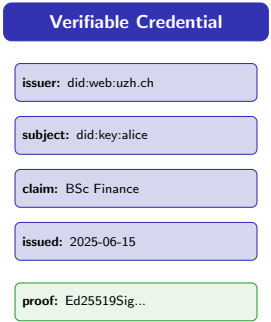
The holder controls when, what, and to whom credentials are shared

What Is a Verifiable Credential (VC)?

A **Verifiable Credential** is a digitally signed statement:

- **Issuer:** "I, the University of Zurich, certify that Alice holds a BSc in Finance"
- **Format:** JSON-LD or JWT (machine-readable)
- **Signature:** Issuer's private key signs the claim
- **Verification:** Anyone can check using the issuer's public key (via the blockchain registry)

Key property: The credential is *tamper-evident* — any modification invalidates the signature.



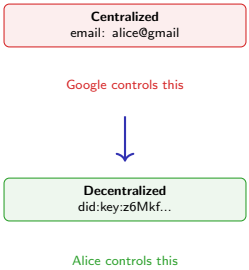
VCs follow the W3C Verifiable Credentials Data Model 2.0 standard — interoperable across wallets and platforms.

What Is a Decentralized Identifier (DID)?

A **DID** is a globally unique identifier that you control:

- Looks like: `did:web:example.com:alice`
- No central registry needed (unlike email or social security numbers)
- Resolves to a **DID Document** containing your public keys
- You can have many DIDs (one per relationship)

Why it matters:
Traditional identifiers (email, phone, SSN) are *assigned* to you. DIDs are *created* by you. No one can take them away.



DIDs are a W3C Recommendation (July 2022) — over 100 DID methods exist, including did:web, did:key, did:ion, and did:ethr.

The Bouncer Analogy: Selective Disclosure

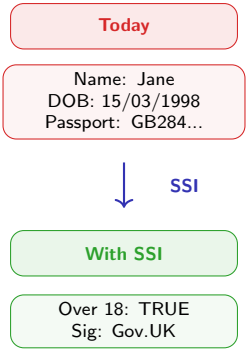
Scenario: You want to enter a bar.

Today:

- You show your passport
- The bouncer sees your name, date of birth, address, nationality, photo, passport number, and expiry date
- The bouncer only *needed* to know: "Over 18? Yes."

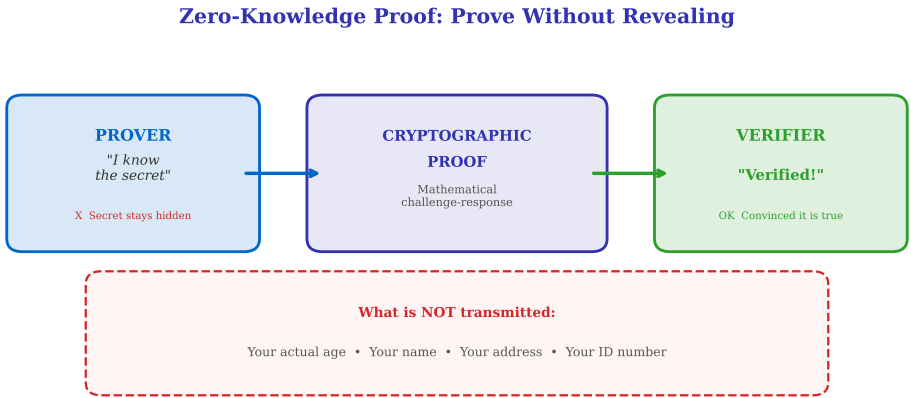
With SSI:

- You present a **derived credential**: "Over 18: TRUE"
- Cryptographically signed by the government
- The bouncer verifies the signature — done
- Your name, birthday, and address stay private



This is "selective disclosure" — reveal only the minimum attributes needed for a given interaction.

Zero-Knowledge Proofs: Prove Without Revealing



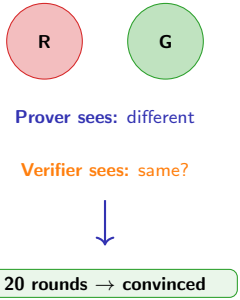
What you see: a three-step flow where the prover convinces the verifier of a fact without transmitting the underlying secret data.

ZKP Intuition: The Color-Blind Friend

Classic analogy:

1. Your friend is color-blind and holds two balls (red and green)
2. He thinks they are the same color
3. You want to prove they are different *without* telling him which is which
4. He hides them behind his back, sometimes swaps, shows you one
5. You always correctly say "swapped" or "not swapped"
6. After 20 rounds, probability of guessing $= \frac{1}{2^{20}} \approx 0.0001\%$

Result: He is convinced the balls are different. He still does not know which is red.



ZKPs in SSI use cryptographic protocols (e.g., BBS+ signatures, zk-SNARKs) rather than interactive rounds, but the principle is identical.

ZKP in Practice: Age Verification

Worked example: Proving you are over 18

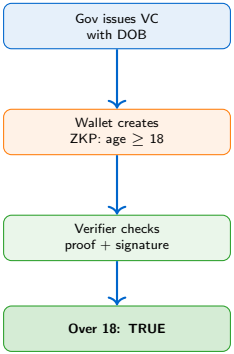
Step 1: Government issues a credential containing your date of birth (e.g., 15/03/2003), signed with their private key.

Step 2: Your wallet computes a ZKP:

- Input: DOB = 15/03/2003, today = 01/04/2026
- Statement: "DOB is before 01/04/2008" (i.e., age $\geq$ 18)
- Output: cryptographic proof (a few hundred bytes)

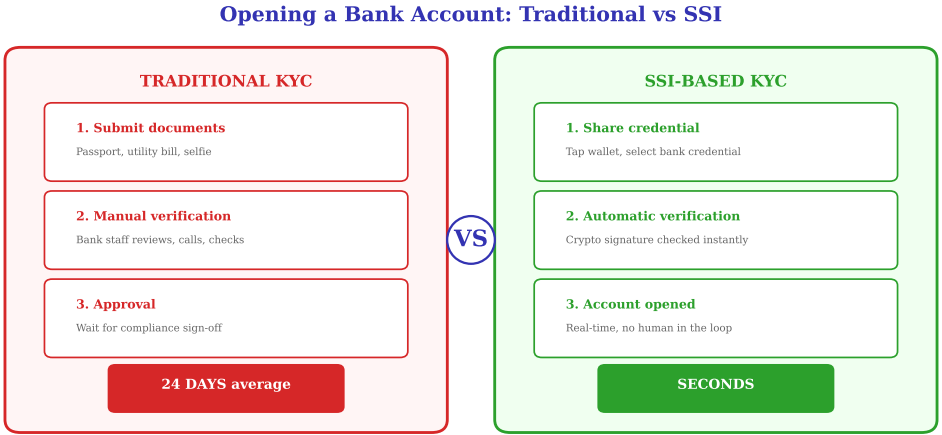
Step 3: Verifier checks the proof against the government's public key.

Result: Verifier knows "over 18 = TRUE." Nothing else.



BBS+ signatures enable selective disclosure natively — you can reveal some fields and hide others from the same credential.

Worked Example: Opening a Bank Account



What you see: traditional KYC takes 24 days average with document uploads and manual review; SSI-based KYC completes in seconds with cryptographic verification.

The KYC Cost Breakdown

Traditional KYC costs per customer:

- Document collection: $15–25
- Manual verification: $20–40
- Compliance officer review: $30–50
- Ongoing monitoring: $10–20/year
- **Total onboarding: $65–115**

Industry total: $60 billion/year globally

SSI-based KYC costs:

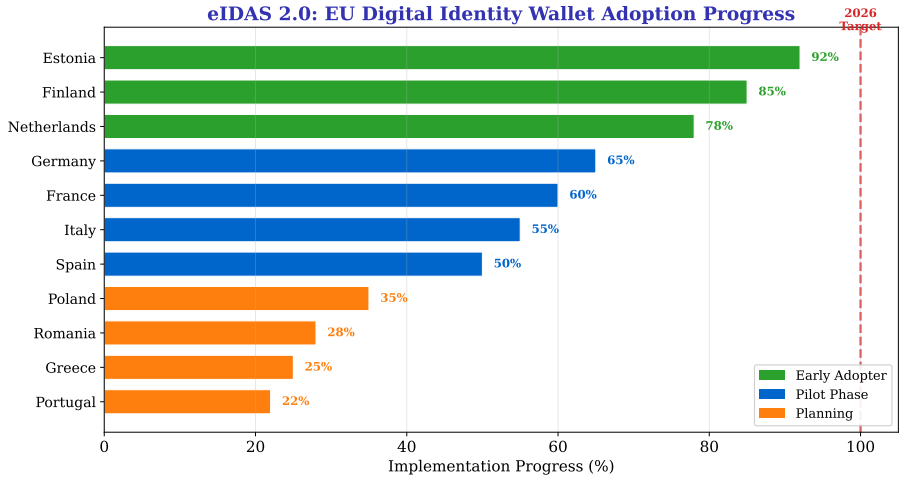
- Credential presentation: $0.01–0.10
- Signature verification: $0.001
- Blockchain DID check: $0.01–0.05
- Ongoing monitoring: automated
- **Total onboarding: $0.02–0.15**

Cost reduction: 99.8%+

But: The issuer (government, university) bears the one-time cost of issuing the credential.
SSI does not eliminate verification cost — it *shifts* it to the issuance stage and *amortizes* it across many verifications.

Cost estimates based on Thomson Reuters KYC Survey (2023) and KPMG Global Banking Report (2024).

eIDAS 2.0: Europe's Big Bet on Digital Identity



What you see: EU member states at different stages of eIDAS 2.0 implementation — Estonia and Finland lead, while Eastern Europe is in the planning stage.

eIDAS 2.0: What It Means for 450 Million Europeans

European Digital Identity Wallet (EDIW):

- Every EU citizen will have access to a digital identity wallet by 2026
- **Cross-border:** a Finnish credential works in Portugal
- **Mandatory acceptance:** banks, telecoms, and public services must accept EDIW
- **Selective disclosure:** share only what is needed
- **No tracking:** issuers cannot track where you use credentials

Scale: 450 million potential users — the largest SSI deployment in history.

Key design choices:

- Wallet app on smartphone
- Government-issued base identity
- Private-sector credentials added (diplomas, bank, health)
- Open standards (W3C, IETF)
- Privacy by design (GDPR-aligned)

Open question: Will governments resist the "no tracking" requirement?

eIDAS 2.0 regulation (EU 2024/1183) entered into force May 2024 — member states have until 2026 to provide wallets.

Think-Pair-Share: University Credentials

Design an SSI system for university credentials.

1. Think (2 min): Who is the issuer? What claims go into the credential? What should students be able to prove?

2. Pair (3 min): Compare with your neighbor. What did you forget? Could a student prove "GPA > 3.5" without revealing exact grades?

3. Share (3 min): Present your design. Can employers verify credentials without calling the university?

Bonus question: what happens when the university shuts down — who maintains the credential's validity?

The SSI Ecosystem: Three Approaches

SSI Ecosystem: Three Approaches

	Government-Led	Crypto-Native	Hybrid
Examples	eIDAS 2.0, Aadhaar	ION, Cheqd, uPort	EU Digital Identity Wallet
Trust Model	State authority	Decentralized consensus	State + open standards
Privacy	Variable (depends on regime)	Strong (zero-knowledge proofs)	Strong (GDPR compliant)
Adoption	Mandatory for citizens	Voluntary, niche communities	Incentivized by regulation
Risk	Surveillance, single point of failure	Key loss, low adoption	Complexity, slow rollout

What you see: government-led (eIDAS, Aadhaar), crypto-native (ION, Cheqd), and hybrid approaches compared on trust model, privacy, adoption, and risk.

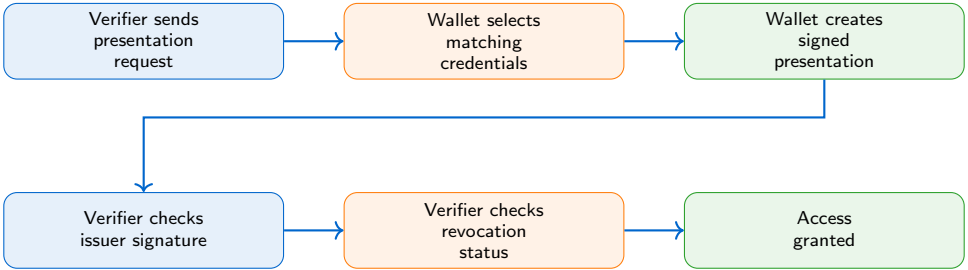
DID Methods: Where Does the Identifier Live?

DID Method	Anchor	Cost	Use Case
`did:web`	Web server (DNS)	Free	Enterprise, eIDAS
`did:key`	Ephemeral (no anchor)	Free	Temporary, testing
`did:ion`	Bitcoin blockchain	$0.01–1	Permanent, public
`did:ethr`	Ethereum blockchain	$0.50–5	DeFi integration
`did:cheqd`	Cheqd network	$0.01	Payment for credentials
`did:sov`	Hyperledger Indy	Free	Enterprise, government

Trade-off: Blockchain-anchored DIDs are censorship-resistant but cost money and are slow. Web-based DIDs are fast and free but depend on DNS (a centralized system).

As of 2025, the W3C DID registry lists 100+ methods — most will not survive; the market is converging on did:web and did:key for enterprise use.

How a Verifiable Presentation Works



Key point: The holder controls the entire flow. The verifier never contacts the issuer directly — there is no "phone home" that would reveal where you use your credential.

Verifiable Presentations wrap one or more VCs with a holder-generated proof, preventing replay attacks and credential theft.

SSI vs Federated Identity ("Login with Google")

Property	Federated (OAuth)	SSI
Who controls data?	Identity provider	**You**
Can provider track you?	Yes (every login)	**No**
Single point of failure?	Yes (account locked)	**No**
Works offline?	No	**Yes** (wallet)
Interoperable?	Vendor-dependent	**Open standards**
Adoption?	**Billions of users**	Early stage
User experience?	**One-click login**	Improving

Key insight: "Login with Google" is convenient but creates a dependency — if Google locks your account, you lose access to every service that relies on it. SSI eliminates this single point of failure.

Federated identity (OAuth 2.0, OpenID Connect) dominates today — SSI must match its user experience to compete.

Hands-On: Trace a Credential Flow

Scenario: Alice graduates from ETH Zurich and applies for a job at UBS.

Trace the flow:

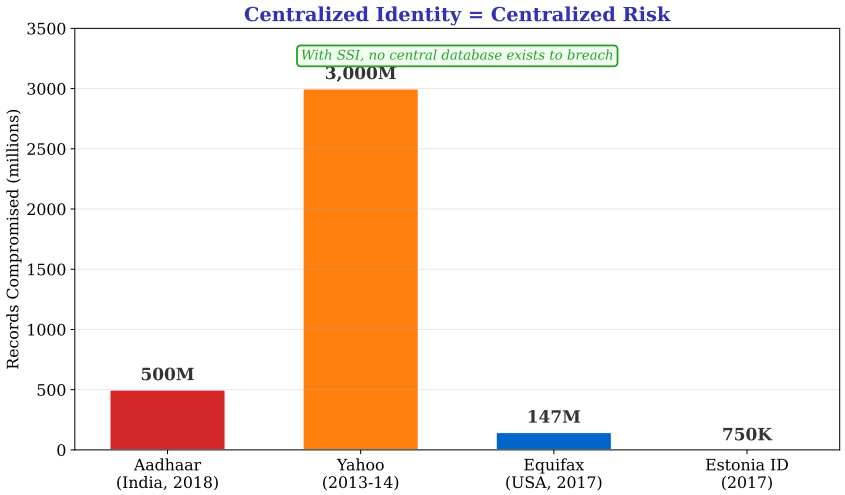
1. ETH issues a VC: "BSc Computer Science, GPA 5.4"
2. Alice stores it in her wallet
3. UBS requests: "Do you have a BSc from a Swiss university?"
4. Alice creates a presentation: "BSc from ETH — TRUE"
5. UBS verifies ETH's signature via the DID registry
6. UBS does **not** learn Alice's GPA, student ID, or enrollment dates

Discussion questions:

- What if UBS also wants to know Alice's GPA?
- Can Alice create a ZKP: "GPA > 5.0" without revealing 5.4?
- What if ETH shuts down — is the credential still valid?
- What if Alice loses her phone?

This exercise maps directly to the eIDAS 2.0 use case for cross-border diploma recognition across the EU.

Centralized Identity = Centralized Risk



What you see: four major breaches — Aadhaar exposed 500M+ records, Yahoo 3 billion, Equifax 147M, Estonia 750K — all because identity data was stored centrally.

Case Study: Aadhaar — 1.4 Billion Identities at Risk

Aadhaar (India, launched 2009):

- World's largest biometric ID system: 1.4 billion enrolled
- 12-digit number linked to fingerprints, iris scans, and photo
- Used for banking, taxes, welfare, SIM cards, and school enrollment

Breaches and concerns:

- 2018: journalists purchased access to the full database for $8
- 500 million+ records exposed across multiple incidents
- No opt-out — if you want government services, you *must* have Aadhaar
- Biometric data cannot be "reset" like a password

SSI alternative:

- Government issues **VCs** instead of storing data centrally
- Citizens hold credentials in wallets
- No central database to breach
- Biometrics stay on device
- Selective disclosure for each service

Trade-off: Aadhaar brought 600 million previously undocumented people into the system. SSI needs device access.

Aadhaar shows the tension: centralized systems achieve massive scale but create massive risk. SSI offers privacy but requires smartphones.

Case Study: Estonia 2017 — When Cryptography Fails

Estonia's e-Residency — the world's most digital government:

- National ID cards with embedded cryptographic chips (Infineon)
- Used for voting, banking, healthcare, and tax filing
- ∼760,000 cards affected (*RIA (Riigi Infosüsteemi Amet / Estonian Information System Authority), ROCA incident reports 2017–18*, 2017) by ROCA (CVE-2017-15361); ∼55% of the adult population
- ROCA: RSA key-gen flaw in Infineon library let private keys be factored from public keys at tractable cost

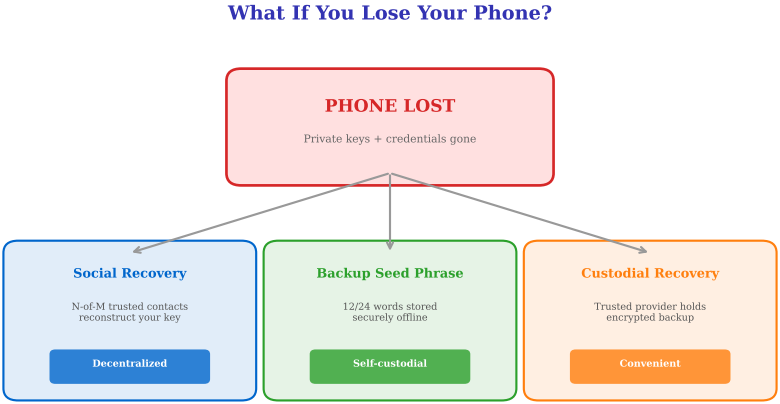
The honest response (not "fixed in weeks"):

- **Nov 3, 2017:** state of emergency declared for ID infrastructure; ∼760K certificates revoked (*RIA announcement Nov 3, 2017; Reuters*, 2017) overnight
- Citizens had to **physically visit police / ID bureaus** to obtain renewed certificates — queues of several hours reported
- Card-crypto functions suspended for ∼4–5 months (*RIA timeline; e-Estonia briefing 2018*, 2017) for the affected cohort
- Direct remediation cost: tens of millions of euros (*Estonian*

Lessons for SSI (revised):

1. Cryptographic algorithms **will** be broken eventually — plan the migration path *before* the break
2. Systems must support **key rotation** and **algorithm agility** end-to-end, not just at issuance
3. A single supply-chain bug (one Infineon library) can compromise an *entire country*'s identity system
4. **The upside of centralization here:** one entity (RIA) could actually coordinate the response. A fully decentralized SSI ecosystem with 10 issuers would have had 10 uncoordinated responses.
5. **The downside:** the response still cost weeks of degraded service and real physical-queue burden on 760K citizens

The Key Management Problem



What you see: three recovery options when you lose your phone — social recovery (N-of-M contacts), backup seed phrase, and custodial recovery.

Key Management: No Perfect Solution

Method	Security	Usability	Decentralization
Seed phrase (12 words)	High	Low	High
Social recovery (3-of-5)	Medium	Medium	High
Cloud backup (encrypted)	Medium	High	Low
Custodial (bank holds key)	Variable	High	None
Hardware wallet (Ledger)	Very high	Low	High

The usability trilemma: You can have at most two of: security, usability, and decentralization.

The reality: Most people will choose the convenient option (cloud/custodial), which reintroduces the centralization that SSI was designed to eliminate.

Key management is SSI's biggest user-experience challenge — if losing your phone means losing your identity, adoption will fail.

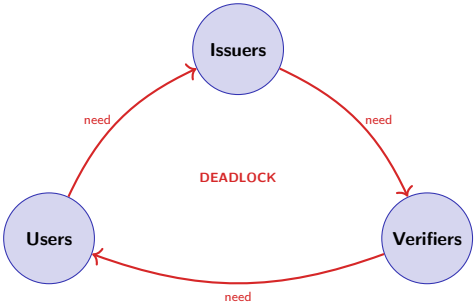
The Chicken-and-Egg Problem

SSI's adoption paradox:

- **Issuers** will not issue VCs until verifiers accept them
- **Verifiers** will not accept VCs until enough people have them
- **Users** will not install wallets until both issuers and verifiers participate

How to break the cycle:

1. **Government mandate** (eIDAS 2.0: banks *must* accept)
2. **Closed ecosystems first** (universities, supply chains)
3. **Dual-mode:** accept both traditional and SSI during transition



eIDAS 2.0 breaks the deadlock by mandating acceptance — this is why government involvement may be necessary despite SSI's decentralization ethos.

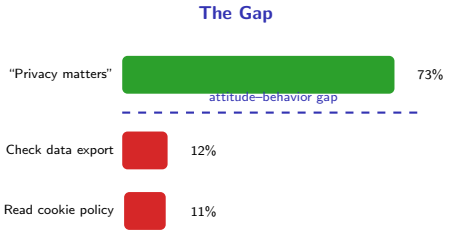
The Privacy Paradox

People say they value privacy but behave otherwise:

- 73% of Europeans say privacy is "very important" (Eurobarometer 2023)
- Yet 89% accept cookies without reading the notice
- 67% use "Login with Google" for convenience
- Only 12% have ever checked their data export from a platform

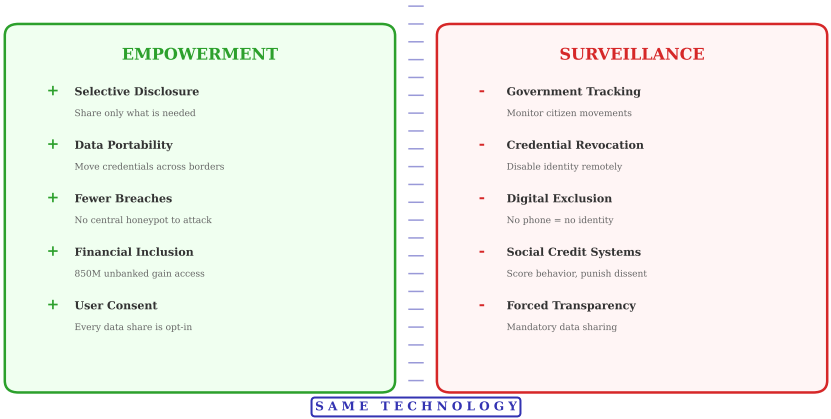
Implication for SSI:
If users do not *perceive* a privacy benefit in their daily lives, they will not switch from convenient centralized systems.

SSI must be easier, not just more private.



The privacy paradox (Acquisti & Grossklags, 2005) is SSI's biggest non-technical barrier — technology alone does not drive adoption.

Digital Identity: Empowerment vs Surveillance



What you see: the same SSI technology enables both user empowerment (selective disclosure, portability) and state surveillance (tracking, revocation) — design choices determine the outcome.

Government vs Self-Sovereign: A Fundamental Tension

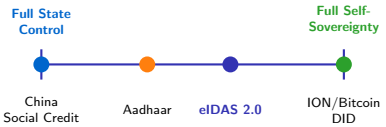
Governments want:

- To know who their citizens are (taxation, law enforcement)
- To revoke credentials of criminals, sanctioned entities
- To ensure compliance with Anti-Money Laundering (AML) rules
- Interoperability with existing legal frameworks

SSI purists want:

- No single entity can revoke your identity
- No tracking of credential usage
- Censorship resistance
- Sovereignty over personal data

eIDAS 2.0 is a compromise: government-issued, user-held, selectively disclosed, but revocable by the state.



No system is purely self-sovereign:

- Even Bitcoin DIDs rely on miners
- Even eIDAS relies on government issuance
- The question is: *where on the spectrum?*

The "self-sovereign" label is aspirational — in practice, all systems involve some trust assumptions and governance.

What Could Go Wrong? A Risk Catalogue

Risk	Impact	Mitigation
Key loss (phone theft)	Total identity loss	Social recovery, backups
Quantum computing	Breaks current crypto	Post-quantum algorithms
Wallet vendor lock-in	New centralization	Open standards, portability
Credential stuffing	Fake credentials	Issuer reputation systems
Regulatory capture	Government overreach	Open-source wallets
User apathy	Low adoption	Better UX, mandates
Phishing attacks	Credential theft	Hardware-bound keys

The meta-risk: SSI replaces a well-understood set of problems (centralized breaches, KYC friction) with a less-understood set (key management, governance, quantum threats). The net risk may not decrease — it *shifts*.

Quantum computers could break RSA and elliptic-curve crypto by 2035 — NIST post-quantum standards (CRYSTALS-Kyber, CRYSTALS-Dilithium) are being finalized.

Discussion: Should Governments Be Able to Revoke Your Identity?

Arguments FOR revocation:

- Criminals should not have valid credentials
- Sanctioned entities must be blocked from financial systems
- Lost/stolen credentials must be invalidated
- Legal frameworks require it (AML, Counter-Terrorism Financing)

Arguments AGAINST revocation:

- Authoritarian regimes could "unperson" dissidents
- Revocation makes SSI no different from centralized ID
- Creates a single point of failure
- Violates the "self-sovereign" principle

Your position: Should eIDAS 2.0 include a government revocation mechanism? Under what conditions? Who decides?

This is not hypothetical — Myanmar's military junta revoked NRC cards of Rohingya minorities, effectively erasing their legal existence.

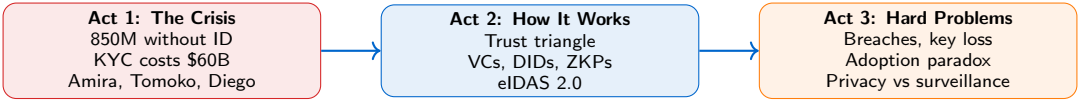
Key Takeaways

1. **Identity is broken:** 850 million lack ID, $60 billion spent on KYC, 300 million records breached annually
2. **SSI puts you in control:** the trust triangle (Issuer → Holder → Verifier) eliminates the need for central databases
3. **Zero-knowledge proofs** enable selective disclosure — prove facts without revealing data
4. **eIDAS 2.0** will bring SSI to 450 million Europeans by 2026 — the largest deployment ever
5. **Key management is the hard problem:** lose your keys, lose your identity
6. **Same technology, different outcomes:** SSI can empower or surveil, depending on who designs the system
7. **Adoption requires convenience:** privacy alone is not enough to drive switching behavior

---

SSI is not a technology problem — it is a governance problem. The technical infrastructure exists; the social infrastructure does not.

What We Covered



The arc: We started with why identity is broken, learned how SSI proposes to fix it, and confronted the problems that remain unsolved.

This lecture connects to Module 8 (Digital Identity in Practice), where we build a working SSI prototype.

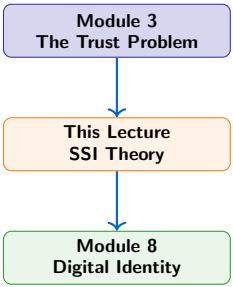
Bridge: From Theory to Practice (Module 8)

What we covered today:

- Why identity is broken (the crisis)
- How SSI works (trust triangle, VCs, DIDs, ZKPs)
- What can go wrong (key management, adoption, surveillance)

What Module 8 will cover:

- Building a digital identity wallet
- Implementing credential issuance and verification
- Testing with real eIDAS 2.0 sandbox environments
- Analyzing privacy vs compliance trade-offs in code



Module 8 is where theory meets code — you will issue, hold, and verify real VCs using open-source toolkits.

Final Discussion

Would you trust a government-issued digital identity?

What if they could revoke it?

1. Would you use a government SSI wallet?

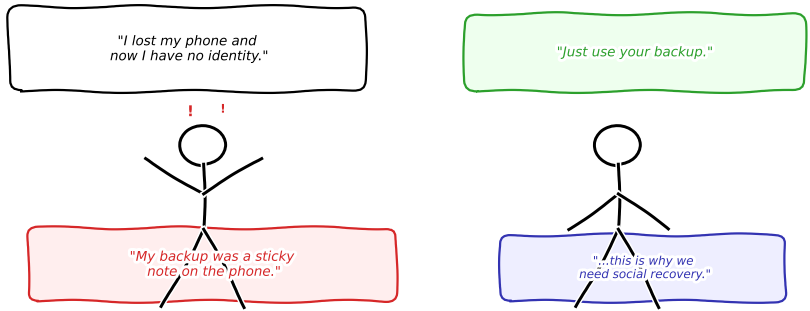
2. What data would you *refuse* to store in it?

3. Should a warrant be required for revocation?

4. Would your answer change if you lived in a different country?

There are no right answers — the point is to recognize that SSI design choices encode political values about privacy, sovereignty, and state power.

Until Next Time



Key management: the hardest unsolved problem in SSI.

Key management: the hardest unsolved problem in SSI — and the reason your mother should not write her seed phrase on a sticky note.

Appendix A: SSI Shifts the Burden — It Does Not Eliminate It

The pitch: "you control your identity." The reality: you inherit responsibilities that a state-backed eID silently handles for you.

What SSI hands you

- Your own key custody — recovery, rotation, revocation
- Your own device security — malware, SIM-swap, phishing
- Your own selective-disclosure decisions — hard UX problem
- Your own trust-list management (which issuers do you trust?)
- Your own cross-border verifier-acceptance uncertainty

Failure modes you absorb

- Lost phone + lost seed = identity locked out
- Estate / incapacity recovery largely unsolved
- No built-in ombudsman; no regulator to call

What a state-backed eID handles for you

- **Recovery infrastructure:** walk into a police station, present biometrics, receive new credential (Estonia, India, Denmark NemID → MitID)
- **Universal verifier acceptance:** every bank, doctor, tax office accepts by statute
- **Legal recourse and liability:** the state is the identity issuer; misbinding is its fault, not yours
- **Revocation on death / incapacity:** integrated with civil registry

Adoption data: Denmark MitID has ∼5M active users (*Digitaliseringsstyrelsen (Danish Agency for Digital Government), MitID annual report 2024*, 2024) (∼99% of adults); Estonia e-ID: >95% of residents (*e-Estonia briefing 2024; RIA*, 2024); EU eIDAS 2.0 wallets mandatory for every member state by 2026. These are real-world, at-scale identity systems — and they are *not* SSI.

Design question for class: for a retiree in rural Finland who loses their phone, which system works better — MitID-style state wallet with a police-station recovery path, or a pure-SSI wallet with a 24-word seed phrase?

Appendix B: Worldcoin / Orb — The Most Consequential SSI Debate of 2024–26

If SSI is about controlling your own identity, Worldcoin is the stress test: scan your iris, receive a unique-human credential ("World ID"), and a token allocation. It is neither obviously SSI nor obviously not.

The proposition

- **Operator:** Tools for Humanity (Sam Altman + Alex Blania, co-founded 2019; token launched Jul 2023)
- **Mechanism:** custom iris-scanning hardware ("the Orb") generates an iris-code hash; binds a World ID credential and distributes WLD tokens to the scanned person
- **Scale:** ~10M+ unique scans across 160+ countries (*Tools for Humanity, Worldcoin progress reports 2024–25*, 2025) — one of the largest biometric-enrollment programs in history

The steelman case

- AI era needs scalable proof-of-personhood to resist bot-generated fraud
- Iris templates stay local to the Orb; only a hash is published
- Open-source protocol (World ID); permissionless verifier integration

Critic positions (2024–26)

- **Kenya:** suspended Aug 2023 pending investigation
- **Germany (BfDI Bavaria):** Dec 2024 order required data-deletion rights
- **Spain / Portugal:** operations suspended by data-protection authorities
- **Hong Kong:** ordered cessation of iris collection 2024
- Biometrics are *irreversible* — a leaked iris template cannot be rotated like a password
- Token-incentive-driven enrollment in low-income regions raises informed-consent concerns

Why this matters for SSI: every SSI framework relies on *some* root attestation that a credential-holder is a unique human. Worldcoin is the most aggressive attempt to supply that root commercially. The regulatory backlash across five

Appendix C: SSI Infrastructure Reality Check

Most of the organisations that built SSI in the 2018–2022 cycle have shut down, pivoted, or quietly wound down. The technology is interesting; the deployments are hard.

The graveyard (2018–2024)

- **Sovrin Foundation:** the original Hyperledger Indy steward; funding crisis 2022–23 (*Sovrin Foundation treasury notices; Indicio blog posts 2023*, 2023), foundation wound down operations, Indy network continued under community stewardship
- **uPort:** pioneering Ethereum-based identity (ConsenSys, 2015); shut down and re-organised into Serto and Veramo (*ConsenSys announcement 2021*, 2021) in 2021
- **Microsoft ION:** Bitcoin-anchored DID network; technically live since 2021, but low enterprise traction; no flagship production identity deployment at scale
- **Canada's Verified.Me:** bank-consortium digital-identity offering; retired / discontinued in 2023 (*Interac / SecureKey announcements 2022–23*, 2023)
- **Estonia e-Residency (the real one):** >100,000 e-resident cards issued (*e-Residency programme annual report 2024*, 2024); active use by businesses materially lower — and issuance dwarfed by resident MitID/eID systems in EU peers

The uncomfortable pattern: what succeeded at scale in digital identity was *state-backed* (MitID, NemID, eIDAS 2.0 wallets, India Aadhaar). What failed at scale was *foundation-led / consortium-led SSI*. Decentralised identifiers (DIDs) are a solid standard; decentralised identity-*issuer* ecosystems have not yet found a commercial model.

Smartphone-exclusion side note: the global unbanked + un-smartphoned population is ∼2.7B people (*GSMA Mobile Economy Report 2024*, 2024). Every smartphone-native SSI design excludes them structurally — the same people the inclusion pitch claims to serve. An honest SSI roadmap must address this. Most do not.

The honest story of 2024–26 is "eIDAS 2.0 mandatory EU wallets are the biggest identity deployment in history, and they are only partially SSI." Read the EU Digital Identity Wallet regulation (EU 2024/1183) for what production-scale identity actually looks like.