Why do you have to prove who you are dozens of times to access financial services that already know you?

The identity verification paradox:

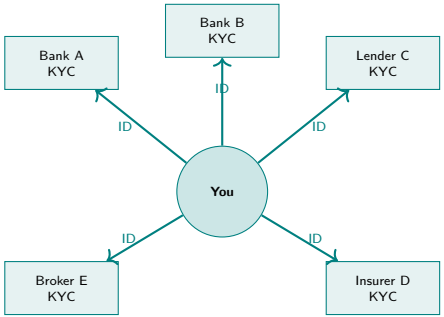
- You prove your identity to open a bank account
- You prove it again to apply for a credit card at the same bank
- You prove it again to get a mortgage from the same institution
- Each time requires documents, delays, and duplicated effort

Why this happens:

- Financial institutions do not share identity data due to privacy laws and competitive concerns
- Each service has its own compliance requirements and cannot trust other systems
- Your identity credentials are locked in institutional silos
- You have no portable proof of who you are

The cost of fragmentation:

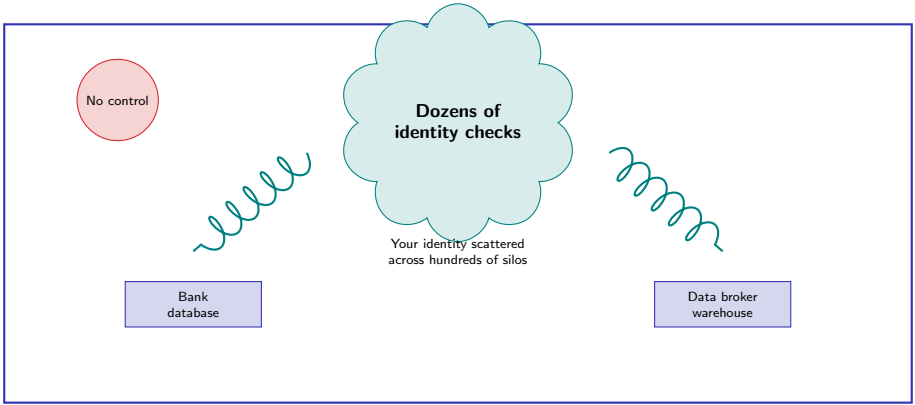
- Consumers spend hours per year on redundant verification
- Institutions spend billions on duplicated identity checks
- People without standard documents are excluded entirely



Same person, dozens of identity checks

Core tension

How many times this month did you verify your identity online – and who stored that data?



Pause and reflect

Count the number of times this month you entered personal information online. Each entry created a copy of your data in a system you do not control.

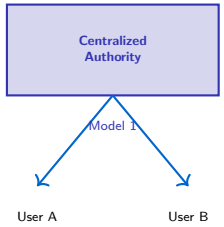
The average person verifies their identity online dozens of times per month, creating hundreds of data copies they cannot monitor, correct, or delete.

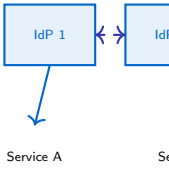
What are the main models for digital identity in financial services?

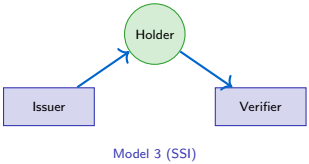
1. **Centralized identity:**
   - A single authority issues, stores, and verifies identity
   - Example: government national ID, bank customer ID
   - Strength: simple, accountable
   - Weakness: single point of failure, no user control

2. **Federated identity:**
   - Multiple providers agree on standards so one credential works across many services
   - Example: Nordic BankID, European eIDAS framework
   - Strength: reduces duplication, interoperability
   - Weakness: provider can track activity, complex governance

3. **Self-sovereign identity (SSI):**
   - The individual holds and controls their own credentials in a digital wallet
   - No central authority required to verify at time of use
   - Strength: user control, portability, minimal disclosure
   - Weakness: high complexity, key management risk







How does a self-sovereign identity system let you prove a claim without revealing the underlying data?

Zero-knowledge proofs (ZKPs) enable selective disclosure:

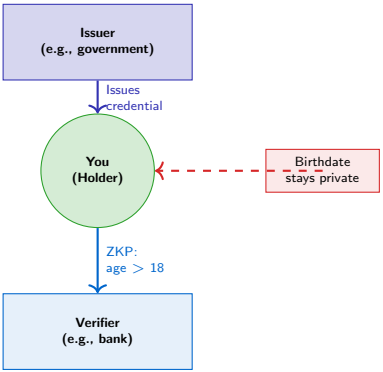
- You can prove you are over 18 without showing your date of birth
- You can prove your income exceeds a threshold without revealing your salary
- You can prove you are not on a sanctions list without revealing all your transactions

How it works (conceptual):

- A trusted issuer signs a credential containing your age
- You hold the credential in a digital wallet
- When a verifier asks for proof of age, your wallet generates a proof that you are over 18 without exposing your exact birthdate
- The verifier checks the cryptographic proof and accepts it

Financial applications:

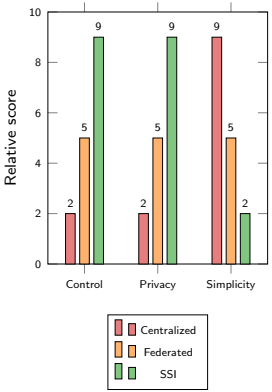
- KYC verification with minimal data exposure
- Credit checks that reveal only pass or fail, not full history
- Accredited investor status without disclosing net worth



Cryptographic foundation

How do centralized, federated, and self-sovereign identity architectures compare?

Attribute	Central.	Feder.	SSI
User control	Low	Medium	High
Single point of failure	Yes	Reduced	No
Privacy	Low	Medium	High
Complexity	Low	Medium	High
Maturity	Mature	Growing	Early



When each model is appropriate:

- Centralized: high-assurance contexts where accountability matters more than privacy (e.g., government ID)
- Federated: cross-border or cross-institution services where convenience outweighs full user control (e.g., Nordic BankID)
- Self-sovereign: contexts where user privacy and control are paramount and users can manage complexity (e.g., financial inclusion for unbanked)

Trade-off pattern

Centralized systems prioritize simplicity at the cost of privacy and control. Self-sovereign systems maximize privacy and control but require users to manage technical complexity.

There is no universally best model: each optimizes for different values and different user populations.

What happens when a centralized identity provider suffers a data breach?

Anatomy of a centralized identity breach:

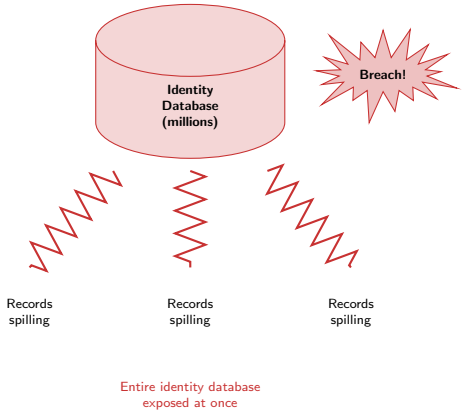
- A single database holds identity data for millions of users
- Attackers compromise the database through a software vulnerability, insider threat, or misconfiguration
- Every user's personal data is exposed simultaneously
- Affected individuals cannot revoke or change their compromised identity attributes

Cascading consequences:

- Identity fraud: attackers open bank accounts, apply for credit, file tax returns using stolen data
- Synthetic identity fraud: combine real and fake data to create new identities
- Reputational damage to the institution
- Regulatory penalties and class-action lawsuits
- Users lose trust in the entire system

Why self-sovereign identity reduces blast radius:

- Credentials are distributed across individual wallets
- No central honeypot database to breach
- Compromising one user does not expose others



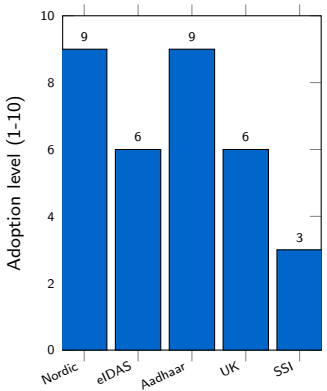
Where are digital identity systems reaching adoption in financial services?

Adoption by geography and model:

Region / System	Model	Adoption
Nordic BankID	Federated	High
EU eIDAS wallet	Federated	Medium
India Aadhaar	Centralized	High
UK Open Banking ID	Federated	Medium
SSI pilots (global)	SSI	Low

Why adoption varies:

- Federated systems benefit from government mandates and institutional coordination
- Self-sovereign systems require user education and wallet adoption
- Network effects favor centralized systems initially but create lock-in



Centralized and federated models dominate today; self-sovereign identity remains in pilot stage.

Adoption pattern

Federated and centralized systems achieve high adoption through institutional coordination and government mandates. Self-sovereign identity faces a bootstrapping challenge.

Who controls your financial identity today and who should control it tomorrow?

Who controls your identity today:

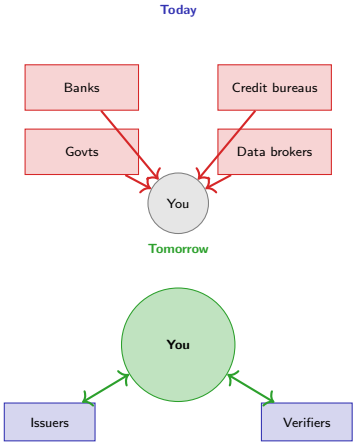
- Banks control your customer identity within their systems
- Credit bureaus control your credit identity and sell access to it
- Governments control your legal identity and grant or revoke it
- Data brokers aggregate fragments and sell profiles
- You have limited visibility and almost no ability to correct errors

Who should control it tomorrow:

- You should hold your own verifiable credentials in a digital wallet
- Issuers (banks, governments) should sign credentials but not store them centrally
- Verifiers should check credentials without storing copies
- You should decide what to share and with whom, on a per-transaction basis

The transition challenge:

- Incumbents profit from data asymmetry and have little incentive to relinquish control
- Regulation can mandate portability but cannot force adoption
- User experience must be seamless or adoption will fail



Power shift

Three questions to evaluate a digital identity system's balance of access and privacy

The Identity System Assessment:

Question 1: Can the user control what data is shared and with whom?

- Does the system allow selective disclosure (e.g., prove age without revealing birthdate)?
- Can the user revoke access to shared credentials?
- Is there an audit log of who accessed the user's data?

Question 2: Does the system work for people who lack traditional identification?

- Can the system accept alternative forms of identity verification?
- Does it support bootstrapping trust through peer attestation or biometric enrollment?
- Is there a path for the unbanked to prove creditworthiness?

Question 3: What is the blast radius of a single-point-of-failure breach?

- How many users are exposed if the central database is compromised?
- Are credentials distributed or centrally stored?
- Can users recover from a breach without system-wide replacement?

Criterion	Score (1-10)
User control	
Selective disclosure	
Inclusion (no-ID users)	
Breach blast radius	
Total	

Scoring guide:

- 1-3: Centralized, institution-controlled
- 4-6: Federated, mixed control
- 7-10: Self-sovereign, user-controlled

Evaluation framework

A balanced identity system maximizes user control and inclusion while minimizing the damage from any single breach.

Your Challenge

Design a KYC process using self-sovereign identity.

Scenario: You are designing the identity verification flow for a new digital bank that serves both traditional customers and the unbanked. The bank must comply with anti-money laundering regulations while maximizing user privacy and inclusion.

Your task:

1. What credentials does the user need to hold in their wallet?
2. Who are the trusted issuers for those credentials?
3. How do you verify the credentials without storing raw personal data?
4. How does the system work for someone who lacks a government-issued ID?
5. What happens if the user loses access to their wallet?

Constraints:

- You must prove the user is not on a sanctions list
- You must establish the user's identity to regulatory standards
- You must allow the user to revoke access to their data at any time
- The system must support users in regions with weak identity infrastructure

Deliverable: Sketch the trust triangle (issuer, holder, verifier) and the credential flow for both a traditional user and an unbanked user.

Think beyond the obvious

Self-sovereign identity is not just about technology. It is about rethinking who holds power in the identity verification process.

This challenge has no single correct answer: it is about balancing regulatory compliance, user privacy, financial inclusion, and technical feasibility.