Prof. Dr. Joerg Osterrieder

Content Reference: Self-Sovereign Identity (SSI)

Digital Finance — BSc Course

Section 1: Key Definitions

- **Self-Sovereign Identity (SSI)** — an identity model in which individuals (not governments or corporations) hold and control their own credentials in a personal digital wallet, disclosing only what each interaction requires.
- **Decentralized Identifier (DID)** — a globally unique, user-generated identifier (syntax `did:method:id`) that resolves to a DID document without a central registry.
- **DID document** — a JSON file containing the public keys, authentication methods, and service endpoints associated with a DID; used by verifiers to validate signatures.
- **Verifiable Credential (VC)** — a digitally signed, tamper-evident claim about a subject (e.g. "Alice holds a BSc from ETH Zurich") issued by a trusted party and stored in the holder's wallet.
- **Zero-Knowledge Proof (ZKP)** — a cryptographic protocol that lets a prover convince a verifier that a statement is true (e.g. "I am over 18") without revealing any underlying data (e.g. date of birth).
- **Selective disclosure** — the ability to reveal only a subset of fields from a credential (e.g. show name but hide address); enabled by BBS+ signatures or SD-JWT.
- **Trust triangle** — the three-party model of SSI: *Issuer* (signs the VC), *Holder* (stores and presents it), *Verifier* (checks the signature); no direct contact between issuer and verifier is needed.
- **Digital wallet** — a smartphone or cloud app that stores DIDs, private keys, and VCs; presents credentials and generates ZKPs on the user's behalf.
- **Revocation registry** — a cryptographic status list (often a bitmap on a blockchain) indicating whether each issued credential is still valid; verifiers check it without contacting the issuer.
- **W3C DID Core specification** — the foundational open standard (Recommendation, 2022) defining the syntax, resolution, and data model for DIDs.

Section 2: Core Concepts

How SSI Actually Works

Trust triangle: *Issuer* signs a credential → *Holder* stores it in a wallet → *Holder* presents a proof to *Verifier*. The verifier trusts the issuer's signature, not the holder's word, and never needs to contact the issuer at verification time.

DID resolution: a DID of the form `did:method:identifier` (e.g. `did:ion:EiA...`) is resolved through its method to a DID document containing the subject's public keys. The verifier uses these keys to check credential signatures.

ZKP age proof: to prove "age ≥ 18" the holder generates a cryptographic proof over the signed date-of-birth field without revealing the date itself. Common constructions: BBS+ signatures, zk-SNARKs (Groth16, PLONK).

Selective disclosure: from a credential with N fields {name, DOB, address, nationality, ...}, the holder reveals exactly the subset a verifier asks for and hides the rest, while the issuer's signature still validates.

Revocation: the issuer publishes a signed status list (e.g. a bitmap at a public URL). Each credential carries an index into that list. Verifiers fetch the list and check the bit; the issuer is never contacted directly.

Section 3: Identity Model Comparison

Model	Data Holder	Trust Anchor	Privacy	Example
Centralized	Single provider	One authority	None	Facebook Login
Federated (SSO)	Identity Provider	IdP + Relying Party	Limited	Google Login, SWITCH edu-ID
Self-Sovereign	User's wallet	Cryptographic proof	Full control	Swiss e-ID, EU Digital Identity Wallet

Section 4: SSI vs Traditional ID

Aspect	Traditional ID	SSI
Data storage	Government / corporate database	User's wallet
What verifier sees	All fields on the ID	Only the required claims
Credential portability	Per-provider	Cross-provider (W3C standard)
Revocation mechanism	Manual re-issue	Real-time status list
User control	None	Full, consent-based
Issuer contact at verification	Required (e.g. call the bank)	Not required

Section 5: Key Facts & Figures

- **W3C DID Core 1.0** — W3C Recommendation (2022); standardises DID syntax, resolution, and the DID document data model.
- **W3C Verifiable Credentials 2.0** — Candidate Recommendation (2024); defines the VC data model, proof formats, and presentation protocols.
- **eIDAS 2.0** (EU Regulation 2024/1183) — mandates an **EU Digital Identity Wallet** for every EU member state, with SSI-style selective disclosure.
- **Swiss e-ID** (federal) — law passed September 2024; launch planned for **2026** on an SSI-based architecture hosted by the Confederation.
- **Sovrin Foundation** — permissioned global public utility ledger for SSI DIDs; sustained volume on the order of hundreds of DID writes per day.
- **Microsoft Entra Verified ID** — enterprise SSI product (launched 2022); issues and verifies W3C VCs for HR, supplier onboarding, and access.

Section 6: Key Risks

1. **Key loss** — a compromised or lost wallet key equals a lost identity; social recovery, MPC, and hardware backups exist but are non-trivial for ordinary users.
2. **Correlation attacks** — if the same DID or signature is reused across verifiers, presentations can be linked; pairwise DIDs and BBS+ signatures mitigate but do not eliminate this.
3. **Issuer centralisation** — governments and banks still issue the underlying credentials; SSI redistributes *storage and disclosure*, not the source of trust.
4. **Verifier coercion** — employers, landlords, or platforms can simply demand more fields than they need; selective disclosure protects privacy only if verifiers do not over-ask.
5. **Standards fragmentation** — W3C VC / DID, ISO 18013-5 mobile driving licence (mDL), and OpenID4VC compete; wallets must often support several stacks.
6. **Digital divide** — SSI requires a smartphone, biometrics, and cryptographic literacy; the very populations that lack ID today (World Bank: ∼850 million) may also lack the devices and skills.

Section 7: Further Reading

- W3C (2022). *Decentralized Identifiers (DIDs) v1.0*, W3C Recommendation.
- W3C (2024). *Verifiable Credentials Data Model v2.0*, W3C Candidate Recommendation.
- European Union (2024). *Regulation (EU) 2024/1183* amending eIDAS (European Digital Identity Framework).
- Sovrin Foundation. *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust* (whitepaper).
- Reed, D., Preukschat, A. (2021). *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*, Manning.