THE LINUX FOUNDATION
OPEN SOURCE SUMMIT
NORTH AMERICA

Embedded Linux Conference

Debunking the Myths of Decentralized Identity

What people get wrong about SSI in 2026
— and what actually matters

Why This Matters Now

- eIDAS 2.0 is in force: every EU member state must offer a digital identity wallet to its citizens
- ~450 million Europeans will receive a wallet; banks, airlines, telcos and public services must accept it
- Apple and Google now support ISO mdoc mobile driving licences across multiple US states and growing
- HAIP 1.0 (Dec 2025) locks down the interop profile for SD-JWT VC + ISO mdoc over OpenID4VC

And yet — the field is buried under misconceptions. Let's clear eight of them.

Eight myths. Ten minutes. Let's go.

Myth 1 — “You need a blockchain”

The reality: decentralized identity is about who controls the credential — not where keys are anchored.

- The EUDI Wallet — the largest SSI deployment in history — uses **no blockchain** in its core architecture
- Trust is anchored in classical PKI and ETSI trust lists (TS 119 612), not a ledger
- DID methods like **did:web**, **did:key**, **did:jwk** don’t require any ledger at all

Decentralization is about control, not consensus.

Myth 2 — “It’s only about Verifiable Credentials”

The reality: VCs is only one of the concepts within Decentralized Identity.

- **Identifiers —** who holds the keys: DIDs (did:web, did:key, did:jwk, did:peer) — and not every flow needs them
- **Verifiable Credentials —** what’s signed: SD-JWT VC, ISO mdoc, W3C VCDM, AnonCreds
- **VC Issuance/Presentation Protocols —** OpenID4VC, DIDComm/Aries, ISO 18013-5/7, ToIP trust-spanning protocol
- **Trust frameworks —** who you believe: trust lists, registries, governance
- **Decentralized protocols** – implement business logic on top of DIDComm or ToIP trust-spanning protocol

VCs ride the stack. The stack — not the VC — is what makes it “decentralized.”

Myth 3 — “It has no real adoption”

The reality: adoption was slow until standards converged in 2023–2024. Now it’s accelerating.

- **EU —** eIDAS 2.0 wallet mandated in every member state by end of 2026;
- **Americas —** BC Gov Person credential and Candy ecosystem (Canada); Gov.br pilots (Brazil)
- **USA —** mDLs in Apple/Google Wallet across a growing list of states (TSA accepts at airports)
- **Asia-Pacific —** Bhutan NDI (full national rollout, 2023); Australia’s myID + Trust Exchange framework
- **Industry (fintech, travel, etc.) —** IATA One ID and Digital Travel Credentials; reusable KYC in production with major IDV vendors

Myth 4 — “One standard” (or: “too many standards”)

The reality: multiple formats AND multiple protocols, by design — with profiles bridging them.

- **VC Formats —** ISO mdoc · SD-JWT VC · W3C VCDM · AnonCreds · KERI ACDC etc.
- **Protocols —** OpenID4VC (HAIP 1.0) · DIDComm / Aries · ISO 18013-5/7 · KERI-native (CESR, IPEX) · ToIP trust-spanning layers

*HAIP 1.0 profiles SD-JWT VC **and** mdoc over OpenID4VC. Pick the right tool for the job — not one stack to rule them all.*

Myth 5 — “Correlation is unavoidable”

The reality: yes, in many flows you’ll be linkable. But the right combination cuts the surface area dramatically.

- **Minimize at presentation —** selective disclosure + tight verifier requests: don’t reveal the attribute, prove a predicate (age > 18)
- **Single-use credentials —** batch issuance gives the wallet many short-lived VCs; a fresh one per verifier blocks signature correlation
- **ZKP layer —** BBS#, longfellow-zk and friends hide the issuer signature itself, breaking the correlation handle entirely
- **No phone-home —** verification uses local trust lists and revocation hints (status lists, CRLs), so the issuer never sees the transaction

Perfect unlinkability is rare. Useful unlinkability is everyday engineering.

Myth 6 — “ZKP requires exotic crypto”

The reality: modern ZKP wraps the standard signatures you already issue — no new HSM, no new format.

- **Google longfellow-zk —** open-source ZK over plain ECDSA-signed mdocs; selective disclosure with no change to the issuer
- **Microsoft Crescent —** ZK proofs over JWTs / SD-JWT VC; same recipe, JSON-friendly credentials
- **BBS# —** multi-message signature scheme designed for unlinkable presentations; standards track at IETF
- **Runs in the secure element —** the underlying issuance signature lives in the phone’s SE; ZKP wraps it client-side, no new hardware

ZKP isn’t a research project anymore. It’s a wrapper around the credentials you’re already issuing.

Myth 7 — “mdoc / OpenID4VC isn’t real SSI”

The reality: the principles — not the labels — are what matter.

- User control, portability, selective disclosure — all delivered by mdoc + OpenID4VC
- EUDI Wallet ships these to 450 million users without DIDComm or a public ledger
- Purist definitions don’t matter to citizens — user data control does
- Gatekeeping the term “SSI” makes the community look out of touch while the rest of the world ships

Stop arguing about labels.

Myth 8 — “No better than federated identity”

Federated (OIDC / SAML)

- IdP must be online at every login
- IdP sees every transaction (the “phone-home” problem)
- All-or-nothing attribute disclosure
- No offline verification
- IdP-held sessions, not user-held

Decentralized (VCs)

- Issuer signs once; offline verification afterward
- Issuer cannot track verifications
- Per-attribute and predicate proofs
- Designed for offline (ISO mdoc)
- User-held credentials in the wallet

What’s Actually True

✓ User control over credentials — real and shipping

✓ Selective disclosure and privacy — real and shipping

✓ Offline verification — real (mdoc)

✓ Standards exist and interoperate (HAIP 1.0)

⚠️ Not a silver bullet — SSI complements, doesn’t replace, federated identity

⚠️ Trust frameworks and governance are the hard part — not the crypto

Thank You

Decentralized identity isn’t a religion, and it isn’t a blockchain product.

It’s a quiet, standards-driven shift in who holds the credential — and that shift is already happening.

Don’t dismiss it because of the hype. Don’t believe everything the hype told you.

Questions?