THE SWISS E-ID

FIVE ANCHORS TO PRESERVE DIGITAL AUTONOMY & DEMOCRATIC SOVEREIGNTY

Christopher Allen — Trust Architect

swiyu 2025-10-02

WHO AM I?

- **Technologist & Trust Architect**
- Co-author of **IETF TLS 1.0** (the 🔒 lock in your browser) in the 1990s

> *"WE BELIEVED THAT TECHNOLOGY COULD PROTECT PEOPLE BY PRESERVING DIGNITY AND AUTONOMY. THAT IT COULD BE A SHIELD AGAINST COERCION, RATHER THAN A CONDUIT FOR IT. THAT IT COULD PRESERVE CHOICE AND AGENCY FOR INDIVIDUALS AND COMMUNITIES. WE WERE WRONG."*

- Originator of **Ten Principles of Self-Sovereign Identity**
- Co-author of the **W3C DID Standard** for decentralized identifiers
- Advisor on **digital identity & digital asset law** in the US & abroad

TLS still secures billions of connections daily, 25+ years later

IMPORTANT CLARIFICATION ON SSI

The Swiss e-ID is NOT *Self-Sovereign Identity*

- **Self-Sovereign Identity**: Citizens control their digital identity infrastructure
    - a focus on personal agency to protect civil and human rights
- **Swiss e-ID**: Government controls issuance, revocation, infrastructure
    - government-managed for institutional trust
    - with democratic oversight
- **This isn't criticism** — it's clarity about what you're building

The Swiss e-ID is a *government digital identity system*.

GOVERNMENT DIGITAL IDENTITY

Swiss Legal Foundation:
Current regulation requires citizens to REQUEST e-ID issuance - voluntary by design.

THE CRITICAL QUESTION:

Can this voluntary principle survive when:

- Private sector creates speed/price advantages for e-ID users?
- Platform dependencies make alternatives second-class?
- Economic reality pressures citizens into "voluntary" adoption?

As other countries learned:

legal voluntary ≠ practical voluntary

HOW "VOLUNTARY" GETS ERODED: INTERNATIONAL CASE STUDIES

Estonia: 99% Adoption Makes Refusal Impractical

- Digital-first government services create speed advantages
- Physical alternatives become second-class citizen experience
- Social pressure: "Everyone has one, why don't you?"
- Result: Legally voluntary, practically mandatory

Ireland: Public Services Card Controversy

- Started voluntary for welfare services
- Gradually required for driver's license, passports, employment
- Citizens forced to choose: get card or lose access to essential services
- Court challenges took years to resolve

India: Aadhaar "Voluntary" Expansion

- Initially voluntary biometric ID for welfare
- Banks, schools, telecom required it for service
- Supreme Court had to intervene to limit scope
- Economic coercion made legal voluntary meaningless

Switzerland's Advantage:

- Democratic institutions can prevent this erosion
- Five Anchors create systematic protection
- Learn from others' mistakes before implementing, not after

The Pattern:

1. Start voluntary with good intentions
2. Private sector creates advantages for adoption
3. Economic pressure makes voluntary meaningless
4. By the time courts intervene, infrastructure dependency is entrenched

INDIVIDUAL AUTONOMY

Personal and family resilience supports choice and agency

- *“I can choose how much to share, when, and with whom.”*
- *“We can protect our family's privacy and security across generations.”*

SWISS DEMOCRATIC SOVEREIGNTY

Constitutional principle that sovereignty resides in the people

- Swiss democratic institutions enable meaningful oversight
- “We collectively govern the systems that govern us”

WHY BOTH MATTER

- Individual autonomy gives substance to democratic sovereignty.
- Without meaningful personal choice, democratic control rings hollow.

These must work together for Swiss e-ID to succeed.

THE SWISS ADVANTAGE

Your democratic institutions can preserve individual autonomy and resilience.

Other countries may copy your technical architecture but lack this governance foundation.

The moment is now: Your referendum has passed.

Choices you make today influence the world for 20 years.

THE TLS WARNING

- We finished **TLS 1.0** in 1996, but only ratified in 1999
- We knew about problems, we thought we'd fix them in **3-5 years**
- Those fixes didn't ship until **TLS 1.3** in 2019 — **20 years later**
- 38% of websites **still** don't use this more secure version
    - More do not fully enable or support all features

Lesson: Once you ship, “good enough” becomes “stuck with it”

FIVE ANCHORS FOR SWISS DIGITAL AUTONOMY

1. **Preserve Choice by Design**
    - Voluntary must mean voluntary-in-practice
2. **Build a 20-Year Architecture, Not 2-Year Product**
    - Infrastructural thinking
3. **Maintain Platform Independence**
    - Resistance to technical capture
4. **Require Duties for Non-Governmental Parties**
    - Private sector accountability
5. **Implement Institutional Safeguards**
    - Democratic oversight of digital power

1) PRESERVE CHOICE BY DESIGN

The Individual Autonomy Anchor

Problem Statement:

Choice disappears when alternatives become second-class

Swiss Reality:

Will the e-ID become mandatory in practice, even if voluntary in law?

1) PRESERVE CHOICE BY DESIGN

How Digital Choice Erodes

Trust builds gradually. Show your age, not your address; your eligibility, not your identity; what's needed now, not everything you have.

This is how physical identity works — digital should match.

You *shouldn't* have to hand over your entire personal profile to be copied just to prove you're over 18.

"WE NOW FACE SYSTEMS THAT PRESUME COMPLIANCE BY DEFAULT AND ELIMINATE MEANINGFUL CHOICE."

1) PRESERVE CHOICE BY DESIGN

Solutions for Meaningful Choice

- **Governance structure with enforcement power:**
  - **Essential service inclusion** — no services (government OR private) limited to digital-only
  - **Economic neutrality** — similar price, speed, dignity for physical alternatives
  - **Legal accountability** — real penalties for coercive practices
- **User-controlled technical architecture:**
  - **Progressive revelation** — citizens control what they share, when, and with whom
  - **Progressive trust UX** — "no, not now, maybe later" instead of "accept or cancel"

1) PRESERVE CHOICE BY DESIGN

Implementation & Enforcement

- **Without enforcement, voluntary becomes meaningless**
- **Need-to-Know schedules**
  - clearly define what data is legitimate for what purposes
- **Hold all sectors accountable**
  - government and private sectors live by similar standards
- **Dark pattern auditing**
  - public transparency on coercive practices

2) BUILD A 20-YEAR ARCHITECTURE, NOT A 2-YEAR PRODUCT

The Infrastructure Anchor

Problem Statement:

MVP thinking optimizes for shipping, not decades of democratic evolution

Swiss Reality:

Democracy moves slowly, technology moves fast — and technical debt can quickly get entrenched

Remember TLS: "Good enough" becomes "stuck with it" for 20+ years

2) BUILD A 20-YEAR ARCHITECTURE

Infrastructural Thinking

- **You're building Switzerland's digital infrastructure, not a startup app**
- **Minimum Viable Architecture, not MVP** — plan now for 20 years, not 2-year shipping
- **Open development practices** — transparency, participation, stewardship
- **Invest in commons** — fund standards participation and library development

2) BUILD A 20-YEAR ARCHITECTURE

Focus on Architectures of Data Minimization

- **Secure data at rest** — transport security alone is insufficient
- **Need-to-Know by design** — technical architecture should enforce legitimate purpose limits
- **Verify and forget capability** — no silent data retention, cross-service linking, or logging of authentication
- **Future-proof selective disclosure** — architecture must support evolving technology
    - SD-JWT + VCs have good intentions for privacy, but called “dead end” by many standards and cryptographic experts
    - *Be prepared to swap it out soon!*

2) BUILD A 20-YEAR ARCHITECTURE

Architectures of Resilience

- **Resilience-first design** — function offline, like physical cards
  - Network failures, emergencies, conflicts cannot disable Swiss identity
  - Maintains Swiss tradition of preparedness and independence
  - *Technical options:* vc-barcodes or animated QRs (QR-UR) for resilient offline verification
- **Technical preparedness**: Prepare for changing to quantum-safe infrastructure now

2) BUILD A 20-YEAR ARCHITECTURE

Swiss Pathway to Greater Autonomy

- **Today**: Government digital identity with democratic safeguards
- **Future**: Start researching alternative models where citizen-control is more appropriate:
    - LESS (legally enabled self-sovereign) Identity
    - State-endorsed but citizen-controlled systems (Utah model)
- **Swiss advantage**: Democratic foundation enables smooth transition

THREE LAYERS OF SWISS DIGITAL SOVEREIGNTY

The next three anchors address different sovereignty vectors:

- **3) Maintain Platform Independence**:
  - TECHNICAL sovereignty (platform infrastructure control)
- **4) Require Duties for Non-Governmental Parties**:
  - COMMERCIAL sovereignty (private sector constraints)
- **5) Implement Institutional Safeguards**:
  - INSTITUTIONAL sovereignty (democratic checks and enforcement)

All are about Swiss digital sovereignty but from different angles of control.

3) MAINTAIN PLATFORM INDEPENDENCE

The Technical Sovereignty Anchor

Problem Statement:

- Dependence on Apple/Google OS app stores
- Government wallets risk becoming surveillance tools
- Platform vendors become unelected gatekeepers of identity

Swiss Reality:
Platforms profit from lock-in, not user autonomy

3) MAINTAIN PLATFORM INDEPENDENCE

The Surveillance Risk

- **Imagine:**
  - Someone gets a ping when your hotel room door opens
  - An accusation of spam disables your Google account, and thus your phone
  - A plagform locks you into their other proprietary services
  - OR, you lose access to these services when you change platforms

If platforms can arbitrarily cut off access,
they control Swiss digital sovereignty!

This must be a line in the sand!

Swiss Principle: Make digital occupation costly and temporary, like the Réduit strategy

3) MAINTAIN PLATFORM INDEPENDENCE

Technical Actions

- **Prohibit platform telemetry** during identity transactions
  - and not just in the e-ID stack!
- **Mandate dignified alternative app distribution**
  - beyond Apple/Google stores
  - accessible to all citizens buying phones retail in Switzerland
- **Require platform accountability —** demand transparency reports on denials of service, timely fixes for critical bugs, etc.
  - *Enforcement mechanism: See Anchor 5, Government Enforcement Capabilities*

3) MAINTAIN PLATFORM INDEPENDENCE

Governance Actions

- **Acknowledge surveillance risks** beyond the e-ID stack
- **Mandate Swiss jurisdiction —** independent oversight with enforcement power

Swiss Reality: This requires contractual obligations, not just technical solutions.

4) REQUIRE DUTIES FOR NON-GOVERNMENTAL PARTIES

The Commercial Sovereignty Anchor

Problem Statement:

- Private sector will likely dominate e-ID usage
- High risk of profiling and surveillance by businesses
- Existing data protection law advises data minimization, however...
    - FADP enforcement fragmented across cantonal prosecutors, lacks consolidated oversight
    - Business surveillance models adapt faster than enforcement can respond
    - Even EU with stronger penalties sees continued massive violations

Swiss Reality:

The bigger risk isn't government surveillance — it's commercial profiling

4) REQUIRE DUTIES FOR NON-GOVERNMENTAL PARTIES

Core Principles

Private sector dominates usage, but no obligations for privacy protection

Your technology choices become theirs — but with different incentives

Required Duties:

- **Purpose limitation** — strict limits to stated business needs
- **Verify and forget** — businesses should not store e-ID data
    - Requires legal reform
    - current liability and retention laws conflict with privacy
- **Unlinkable** — no silent pings, no tracking across services

4) REQUIRE DUTIES FOR NON-GOVERNMENTAL PARTIES

Private Sector Accountability

- **Temporary storage only** — default to immediate deletion
- **Best practices defined** — clear guidance, lose trusted status if caught profiling
- **Public transparency** — audit and publish violations

Reality: Business adoption will be rapid — rules must be ready before widespread use.

5) IMPLEMENT INSTITUTIONAL SAFEGUARDS

The Democratic Sovereignty Anchor

Problem Statement:

- **Revocation power concentrated** — Office of Police can disable citizen's digital access
- **Administrative separation only** — appeals handled by different office, but same Federal Councilor (Beat Jans)
- **No guaranteed human review timeframes** — citizens may be locked out indefinitely
- **What happens when political winds change?** — both offices under same political leadership

Swiss Principle: Sovereignty resides in the people

The Balance:

Swiss democracy requires both empowering government to protect citizens from private sector abuse AND constraining government overreach.

5) IMPLEMENT INSTITUTIONAL SAFEGUARDS

Revocation Safeguards

- **Two-party authorization required** — no single office can revoke e-ID credentials
- **Mandatory court review within 48 hours** — judicial oversight of revocation decisions
- **Automatic temporary restoration pending appeal** — citizens not locked out during review
- **Public transparency reports** — revocation statistics, reasons, and appeal outcomes published quarterly

5) INSTITUTIONAL SAFEGUARDS

Political Independence

- **Independent oversight authority** — reports to Parliament, not Federal Councilor
- **Cross-party appointment process** — prevents single-party control of digital rights
- **Fixed terms with cause-only removal** — insulates from political pressure
- **Separate data governance** — government departments cannot share e-ID transaction data

5) IMPLEMENT INSTITUTIONAL SAFEGUARDS

Institutional Enforcement Capacity

- **Guaranteed human review across all sectors** — no automated denials of core rights by government or private entities
- **Clear explanations required** — citizens deserve to know why decisions were made
- **Service level commitments** — response times guaranteed by law
- **Sustained enforcement budget** — 20-year capacity to investigate and remedy violations
- **Cross-agency coordination** — institutional framework to enforce all five anchors

THE VISION: SWISS DIGITAL AUTONOMY

Success Looks Like:

- **Choice preserved:** Digital and physical options remain equivalent
- **Architecture sustainable:** 20-year thinking, not 2-year shipping
- **Technical sovereignty maintained:** Platform independence with democratic oversight
- **Commercial sovereignty secured:** Businesses verify and forget, not profile and hoard
- **Institutional sovereignty protected:** Appeals, explanations, and human review guaranteed

This reflects one fundamental principle…

THE RIGHT TO REFUSE

The Foundation:

> *"If a system cannot hear you say no, it was never built for **us**. It was built for **them**."*

The Swiss e-ID must preserve the right to refuse — that's what makes it Swiss

Because in Switzerland, sovereignty resides in the people.

Your digital identity must reflect this constitutional principle: you delegate authority to systems, but you never surrender it.

THANK YOU!

Christopher Allen *<ChristopherA@LifeWithAlacrity.com>*

Available for policy review, technical consultation, and trust architecture

- ***Schedule with me***:
  - Technical deep-dive on complexities of minimal and selective disclosure
  - Moving toward alternative models:
    - LESS (legally enabled self-sovereign) Identity
    - State Endorsed Identity (Utah is exemplar)
  - UX issues and Progressive Trust prototypes
  - Threat-model wallet designs for Swiss democratic values