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*.

ANNOTATION: WHAT IS SELF-SOVEREIGN IDENTITY? (1/3)

Self-Sovereign Identity Definition:

- Individual controls their own digital identity and credentials
- No central authority required for identity verification
- Citizens own their data and decide what to share, when, and with whom
- Identity works across different services and platforms

Key SSI Characteristics:

- **Decentralized**: No single point of control or failure
- **Portable**: Identity works everywhere, not locked to one service
- **Private**: Minimal disclosure of personal information
- **Persistent**: Identity survives even if organizations disappear

ANNOTATION: TEN PRINCIPLES OF SELF-SOVEREIGN IDENTITY (2/3)

Christopher Allen's Ten Principles (2016):

1. **Existence**: Users must have an independent existence
2. **Control**: Users must control their identities
3. **Access**: Users must have access to their own data
4. **Transparency**: Systems must be transparent
5. **Persistence**: Identities must be long-lived
6. **Portability**: Information must be transportable
7. **Interoperability**: Identities should be widely usable
8. **Consent**: Users must agree to the use of their identity
9. **Minimalization**: Disclosure should be minimized
10. **Protection**: Users' rights must be protected

ANNOTATION: WHY SWISS E-ID USES SSI TECHNOLOGY DIFFERENTLY (3/3)

Key Differences:

- **SSI**: Citizens control issuance, revocation, and infrastructure
- **Swiss e-ID**: Government controls issuance, revocation, and infrastructure
- **SSI**: No central authority required
- **Swiss e-ID**: Government serves as trusted central authority

Why This Distinction Matters:

- Different governance requirements for government vs. citizen-controlled systems
- Understanding the architecture helps design appropriate democratic safeguards
- Clarifies what you're actually governing and how to do it effectively

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."*

ANNOTATION: SWISS DIGITAL SERVICE EROSION EXAMPLES (1/3)

International Context:

- Banking sector globally shifting to digital-first with physical branch closures
- Government services worldwide adopting "digital by default" policies post-COVID
- Payment systems transitioning from cash-optional to digital-preferred models

Problems/Issues:

- **Swiss banking consolidation**: UBS closing 85 branches (1/3 reduction) by 2025 after Credit Suisse merger
- **Government service digitization**: easyGov platform expanding, QES signatures required for employment contracts
- **Payment infrastructure shift**: TWINT now accepted by 81% of stores, creating speed/convenience advantages over cash

ANNOTATION: DIGITAL SERVICE EROSION IMPACT ANALYSIS (2/3)

Implications:

- Legal voluntary status maintained while practical voluntary erodes through convenience and scarcity
- Citizens face increasing economic pressure to adopt digital services for basic needs
- Physical alternatives becoming second-class through reduced availability and efficiency
- **Swiss Choice Point**: This pattern can be prevented through proactive design, not just accepted as inevitable

ANNOTATION: SWISS CHOICE PRESERVATION OPPORTUNITY (3/3)

Swiss Application:

- e-ID risks following same pattern: legally voluntary, practically mandatory within 5-10 years
- Current digitization trends demonstrate both the risk and the opportunity for intervention
- Swiss democratic advantage: institutions can enforce meaningful choice preservation where other countries cannot
- Swiss scale enables maintaining dignified alternatives if designed systematically from the start

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"

ANNOTATION: PROGRESSIVE TRUST IMPLEMENTATION MODELS

Progressive Trust Success Cases:

- Apple's "Ask App Not to Track" — simple, clear choice without penalties
- GDPR consent interfaces (when done right) — granular, revocable permissions
- Swiss banking: graduated disclosure for different transaction types

Progressive Trust Design Principles:

- "No, not now, maybe later" instead of "accept or cancel"
- Citizens control what they share, when, and with whom
- Trust builds gradually through voluntary interactions
- Physical identity model: show age not address, eligibility not full identity

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

ANNOTATION: MVA VS MVP - ARCHITECTURAL DESIGN (1/3)

International Context:

- **US Federal Government**: $7 billion technical debt from MVP-style decisions that became permanent
- **TLS/SSL success**: Modular plug-in architecture enabled 25+ years of cryptographic evolution
- **Estonia e-ID**: Successful but locked into specific technical choices, difficult to evolve

Problems/Issues:

- **MVP approach** optimizes for immediate shipping, creates inflexible technical debt
- "Good enough" solutions become permanent when replacement costs are prohibitive
- Architectural decisions lock governments into specific vendors and technologies for decades

ANNOTATION: MVA RESEARCH FOUNDATION (2/3)

Core MVA Principle:

- **Quote from MVA research**: "We don't always know the right solutions… the best we can do is create architectures that won't lock us in to specific decisions about the future"

Implications:

- Swiss e-ID architectural choices will constrain democratic evolution for 20+ years
- MVP thinking creates competitive vulnerabilities and limits future innovation
- Without modular design, Switzerland becomes dependent on current technology assumptions

ANNOTATION: SWISS MVA IMPLEMENTATION STRATEGY (3/3)

Swiss Application:

- **MVA principles**: "Hollow out spaces in architectures for future development"
- **Modular and expandable design**: Separate core identity specifications from implementation details
- **Swiss open source strategy**: EMBAG law enables collaborative "coopetition" development
- **Architectural flexibility**: Design identity system to accommodate future, currently unanticipated developments
- **Democratic timeline advantage**: Switzerland can afford slower, more thoughtful architectural choices that serve 20-year democratic evolution

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!*

ANNOTATION: SD-JWT CRITICAL ASSESSMENT (1/3)

International Context:

- Hash-based selective disclosure provides solid privacy foundation for digital credentials
- SD-JWT represents one specific implementation approach with known limitations
- Cryptographic experts have identified significant architectural constraints in current SD-JWT specification

Problems/Issues:

- **Rigid Structure**: Hard-coded format makes evolution difficult for 20-year systems
- **No Unlinkability**: Signatures correlate across different verifications, limiting privacy
- **Cryptographic Lock-in**: Each new crypto method requires rebuilding entire payload structure

ANNOTATION: EXPERT CONSENSUS ON SD-JWT LIMITATIONS (2/3)

Expert Assessment:

- **Expert Consensus**: Multiple cryptographic specialists note these as "serious flaws" for long-term deployment

Implications:

- BBS+, zero-knowledge proofs, other advances require complete reimplementation in SD-JWT
- Cannot evolve cryptographically without replacing entire credential format
- A 20-year timeline exposes these architectural limitations more than short-term deployments

ANNOTATION: SWISS ARCHITECTURAL DECISION POINT (3/3)

Swiss Application:

- Switzerland's democratic deliberation advantage allows time to address these architectural issues
- Better architectural approaches exist that preserve privacy benefits with more flexibility
- Swiss technical choices will influence global democratic digital identity for decades
- **Critical Decision Point**: SD-JWT's architectural limitations conflict with Swiss 20-year infrastructure requirements

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

ANNOTATION: SWISS RESILIENCE INFRASTRUCTURE MODELS (1/3)

International Context:

- **Alpine data centers**: Swiss providers embed infrastructure deep in solid rock for physical protection
- **Geographic redundancy**: Swiss cloud systems maintain copies in both Zurich and Geneva (100km+ separation)
- **Telecommunications resilience**: Dual fiber paths and automatic failover systems across Switzerland

Problems/Issues:

- Digital identity systems typically have single points of failure
- Network dependencies make government services vulnerable during emergencies
- Most identity systems cannot function without internet connectivity
- Physical verification often unavailable when digital infrastructure fails

ANNOTATION: EMERGENCY RESILIENCE REQUIREMENTS (2/3)

Implications:

- Swiss preparedness traditions require digital systems to match physical resilience standards
- Emergency situations expose critical infrastructure vulnerabilities
- Citizens lose access to essential services during network disruptions
- Network failures, emergencies, conflicts cannot disable Swiss identity

Swiss Preparedness Heritage:

- **Physical resilience tradition**: 7,200 emergency sirens, universal bomb shelters, wired mountain defenses
- **Historical emergency examples**: Japan 2011 tsunami (digital systems failed, physical ID cards enabled evacuation), Puerto Rico 2017 hurricane (power out for months), Texas 2021 winter storm (digital infrastructure disabled)

ANNOTATION: OFFLINE INDEPENDENCE IMPLEMENTATION (3/3)

Swiss Application:

- **Technical implementation requirements**: Physical verification must work when digital infrastructure fails
- **Emergency preparedness integration**: Digital identity systems must function during natural disasters
- **Emergency ID models**: California's Instant Identity Card for wildfire victims - enables immediate access to services when documents destroyed
- **Swiss Emergency models**: Identity verification needed after earthquake, flood, landslide, without network connectivity
- **Offline-first architecture**: QR codes and cryptographic signatures working without network connectivity
- **Swiss preparedness culture**: "Trust but verify" includes verifying systems work when infrastructure fails

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

ANNOTATION: GOVERNMENT-TO-CITIZEN IDENTITY EVOLUTION MODELS (1/2)

International Context:

- **Utah model**: State-endorsed but citizen-controlled digital identity systems
- **Estonia lessons**: Government e-ID success but limited citizen control over long-term evolution
- **LESS Identity research**: Legally Enabled Self-Sovereign Identity as bridge between government and citizen control

Problems/Issues:

- Government-issued digital identity can become government-controlled digital identity
- Citizens have limited input on long-term digital identity system evolution
- Technical choices made for government convenience may conflict with citizen autonomy

ANNOTATION: GOVERNMENT-TO-CITIZEN IDENTITY EVOLUTION MODELS (2/2)

Implications:

- Democratic institutions need pathways to evolve toward greater citizen control
- Switzerland's federal structure enables gradual autonomy increases
- Technical architecture today determines citizen empowerment possibilities for decades

Swiss Application:

- **Swiss democratic foundation**: Federal system with cantonal experimentation enables smooth transitions
- **Phase 1**: Government digital identity with strong democratic safeguards (current e-ID implementation)
- **Phase 2**: Research LESS Identity models with state endorsement but citizen control
- **Phase 3**: Evaluate full citizen-controlled systems based on democratic feedback and technical maturity
- **Swiss advantage**: Democratic institutions can manage identity evolution better than authoritarian or purely market-driven systems

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

ANNOTATION: DIGITAL WALLET IMPLEMENTATION RISKS AND SWISS ADVANTAGES (1/2)

International Context:

- **EU Digital Identity Wallet**: Privacy advocates warn of "farming citizen data" by governments and corporations
- **Japan My Number Card**: 80% of citizens distrust government's ability to protect digital ID information
- **Singapore/Nigeria**: Elderly populations locked out of services due to biometric system failures

Problems/Issues:

ANNOTATION: DIGITAL WALLET IMPLEMENTATION RISKS AND SWISS ADVANTAGES (2/2)

Implications:

- Digital identity architectures require careful design to prevent misuse
- Even well-intentioned systems can be repurposed by future administrations
- Switzerland's international reputation creates responsibility for democratic digital identity models

Swiss Application:

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*

ANNOTATION: PLATFORM ALTERNATIVE IMPLEMENTATION MODELS (1/2)

International Context:

- **Japan's App Store Law**: Forces Apple/Google to allow third-party app stores and payment systems
- **EU Digital Markets Act**: Requires "gatekeeper" platforms to allow alternative distribution methods
- **F-Droid Model**: Open-source app distribution used by privacy-focused European governments

Problems/Issues:

- Platform gatekeeping prevents government control over critical identity infrastructure
- Native app dependencies create single points of failure for national services
- Platform updates can break government functionality without warning or consent

ANNOTATION: PLATFORM ALTERNATIVE IMPLEMENTATION MODELS (2/2)

Implications:

- Swiss digital sovereignty requires technical independence from foreign platforms
- Citizens need guaranteed access regardless of corporate platform decisions

Swiss Application:

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.

ANNOTATION: SWISS JURISDICTION ENFORCEMENT MODELS (1/2)

International Context:

- **UK Competition Authority**: Forcing platform openness through market power investigations
- **EU GDPR**: Extraterritorial jurisdiction compelling foreign company compliance
- **China Cybersecurity Law**: National data sovereignty requirements overriding platform terms

Problems/Issues:

- Platform terms of service currently override Swiss law in practice
- No direct government leverage over platform operational decisions affecting citizens
- Swiss courts cannot enforce decisions against foreign platform companies

ANNOTATION: SWISS JURISDICTION ENFORCEMENT MODELS (2/2)

Implications:

- Platform control over identity infrastructure undermines democratic sovereignty
- Citizens have no legal recourse when platforms restrict government service access

Swiss Application:

- **Government procurement power**: Require Swiss jurisdiction compliance for public contracts
- **Market access requirements**: Platform services must accept Swiss legal authority
- **Financial penalties**: Sanctions must be sufficient to change corporate behavior (not token fines)
- **Service guarantee bonds**: Platforms post collateral ensuring continued service availability

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

ANNOTATION: SWISS FADP VS EU GDPR ENFORCEMENT REALITY (1/2)

Swiss FADP Enforcement Gaps:

- No direct fining power for Federal Data Protection Commissioner (FDPIC)
- Enforcement scattered across 26 cantonal prosecutors
- Maximum fines CHF 250,000 vs GDPR's 4% global revenue
- FDPIC can only "file grievances" and "participate as private plaintiff"

EU GDPR Despite Strong Penalties:

- €5.88 billion in cumulative fines by 2025
- Meta alone fined €1.2 billion in January 2025
- Yet surveillance capitalism business models persist and adapt
- Some member states create "regulatory safe zones"

ANNOTATION: SWISS FADP VS EU GDPR ENFORCEMENT REALITY (2/2)

Business Intelligence Reality:

- Hotels, employers, landlords will use e-ID daily for verification
- Without clear rules, becomes profiling and tracking goldmine
- Current retention laws actually conflict with privacy goals
- "Verify and forget" requires legal reform, not just technical solutions

Private Sector Economic Coercion Patterns:

- Airlines charging "paper ticket fees" for non-digital transactions
- Banks requiring smartphone apps for basic services access
- Apartment rentals demanding "digital verification only" creating housing discrimination
- E-ID verification becoming defacto requirement for employment, services, housing

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

ANNOTATION: TECHNICAL IMPLEMENTATION OF "VERIFY AND FORGET" (1/2)

International Context:

- **Zero-Knowledge Proofs**: Google's open-source ZKP for EU age verification without revealing birthdates
- **Differential Privacy**: US Census Bureau injects noise to protect individuals while releasing statistics
- **Privacy-Preserving Credentials**: Systems enable age verification without disclosing unnecessary personal data

Problems/Issues:

- Most business verification systems store complete credential data permanently
- "Verify and forget" lacks standardized technical implementation models
- Current Swiss retention laws conflict with privacy minimization goals
- Businesses have economic incentives to retain data for profiling

ANNOTATION: TECHNICAL IMPLEMENTATION OF "VERIFY AND FORGET" (2/2)

Implications:

- Without technical enforcement, "verify and forget" becomes voluntary compliance theater
- Swiss e-ID could become business intelligence goldmine without architectural protection
- Legal requirements need technical implementation standards to be enforceable

Swiss Application:

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.

ANNOTATION: INTERNATIONAL BUSINESS ACCOUNTABILITY MODELS (1/2)

International Context:

- **Singapore Singpass**: 97% citizen adoption, 1,700+ private sector services with government oversight
- **UK Digital Identity Framework**: 34% of firms international, strict accountability standards
- **GDPR enforcement**: €5.88 billion in fines, but Meta still paid €1.2 billion and continued surveillance practices

Problems/Issues:

ANNOTATION: INTERNATIONAL BUSINESS ACCOUNTABILITY MODELS (2/2)

Implications:

- Swiss e-ID private sector adoption will be rapid but accountability frameworks lag behind
- Without proactive accountability, businesses will optimize for data collection
- International experience shows fines alone insufficient to change behavior

Swiss Application:

- **Preventive accountability**: Regular audits and published violation reports before problems escalate
- **Trusted status system**: Clear guidance with loss of trusted verifier status for profiling violations
- **Real-time monitoring**: Automated compliance monitoring rather than reactive investigation
- **Swiss procurement leverage**: Government contract requirements for private sector accountability standards
- **International cooperation**: Learn from Singapore's oversight model while maintaining Swiss privacy standards

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.

ANNOTATION: SWISS FEDERAL AUTHORITY STRUCTURE & INTERNATIONAL SAFEGUARDS (1/2)

Current Swiss Structure (per Rolf Rauschenbach):

- Federal Office of Police: e-ID issuance and revocation
- Federal Office of Justice: appeals for overidentification, impersonation, illegitimate use
- Both offices under Federal Department of Justice and Police (FDJP)
- Both report to same Federal Councilor: Beat Jans
- Third office (FOITT) runs infrastructure but limited authority over policy

Revocation Risks:

- Immediate loss of access to e-ID dependent services
- Could affect housing, employment, banking if private sector adopts widely
- Appeals process may be too slow for time-sensitive needs
- Political pressure could influence both issuance and appeals

ANNOTATION: SWISS FEDERAL AUTHORITY STRUCTURE & INTERNATIONAL SAFEGUARDS (2/2)

International Separation Models:

- UK: Independent Information Commissioner separate from government departments
- Germany: Federal Commissioner for Data Protection reports directly to Parliament
- Canada: Privacy Commissioner independent from executive branch
- Estonia: e-Residency appeals handled by courts, not administrative offices

Revocation Safeguards (Other Countries):

- Two-party authorization required for revocation
- Mandatory court review within 48 hours
- Automatic temporary restoration pending appeal
- Public transparency reports on revocation statistics and reasons

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

ANNOTATION: INTERNATIONAL ENFORCEMENT MODELS (1/3)

International Service Protection Models:

- **Germany**: Onlineausweis-Gesetz requires government services maintain offline alternatives
- **Canada**: Digital Charter ensures "right to disconnect" from digital services
- **EU Accessibility Directive**: Physical access required alongside digital services

Cross-Sector Enforcement Authority:

- **EU GDPR**: €5.88 billion in fines across government and private violations
- **UK ICO**: Authority over both public and private sector data processing
- **Australian Privacy Commissioner**: Oversight of government agencies and businesses

ANNOTATION: ENFORCEMENT REALITY REQUIREMENTS (2/3)

Enforcement Effectiveness Standards:

- **Real penalties**: Without substantial sanctions, voluntary compliance becomes theater
- **Legal binding standards**: Need-to-Know schedules must be legally enforceable, not suggestions
- **Systematic auditing**: Dark pattern detection requires dedicated resources and public transparency
- **Cross-sector accountability**: Government and private sectors held to equivalent standards

ANNOTATION: SWISS INSTITUTIONAL CAPACITY FRAMEWORK (3/3)

Swiss Institutional Capacity Requirements:

- **Human Review Guarantees**: No automated denials of core rights by any sector
- **Service Level Commitments**: GDPR-style "without undue delay" response requirements with specific timeframes
- **20-Year Sustainability**: Independent budget allocation prevents political defunding
- **Professional Standards**: Career protection for oversight personnel ensures institutional memory
- **Democratic Accountability**: Treaty-level commitments ensure sustained enforcement capacity

ANNOTATION: INTERNATIONAL REVOCATION SAFEGUARDS EXAMPLES (1/2)

Two-Party Authorization Models:

- US Data Protection Review Court: Two-level redress mechanism with independent review
- EU GDPR: Supervisory authorities require transparent procedures for appointment/dismissal
- Australia: Draft legislation prevents law enforcement access without warrant

Court Oversight Examples:

- Sri Lanka: District-level Registration of Persons Tribunals for ID card appeals
- US DPRC: Independent court reviews intelligence agency determinations
- EU: Court of Justice emphasizes independent authority control as "essential component"

ANNOTATION: INTERNATIONAL REVOCATION SAFEGUARDS EXAMPLES (2/2)

Automatic Restoration Practices:

- EU institutions: DPOs cannot be dismissed without EDPS consent
- GDPR: Dismissal only for "serious misconduct" or failing to meet qualifications
- Fixed terms (3-5 years) with limited removal grounds

Transparency Requirements:

- GDPR requires transparent appointment procedures to minimize political influence
- Philippines: Legislation prevents sharing personal information with third parties
- Brazil: Digital ID adopted through legislative reform, not executive action

ANNOTATION: INDEPENDENT OVERSIGHT: INTERNATIONAL MODELS (1/2)

Appointment Process Best Practices:

- EU: Transparent procedures, professional qualifications, experience requirements
- Cross-party involvement prevents single-party control
- Independent from "any direct or indirect external influence" (GDPR standard)

Fixed Term Protections:

- EU institutions: 3-5 year terms, reappointment possible
- Dismissal only with consent of independent authority (EDPS model)
- "Complete independence" with decision-making power free from external influence

ANNOTATION: INDEPENDENT OVERSIGHT: INTERNATIONAL MODELS (2/2)

Structural Independence Examples:

- EU Data Protection Authorities: Independent from three branches of government
- UK Information Commissioner: Reports to Parliament, not executive
- German Federal Commissioner: Direct parliamentary reporting relationship

Resource Protection:

- GDPR requires "sufficient resources" allocation
- Independent budget authority prevents political pressure through funding
- "Meaningful decisions without external interference" standard

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