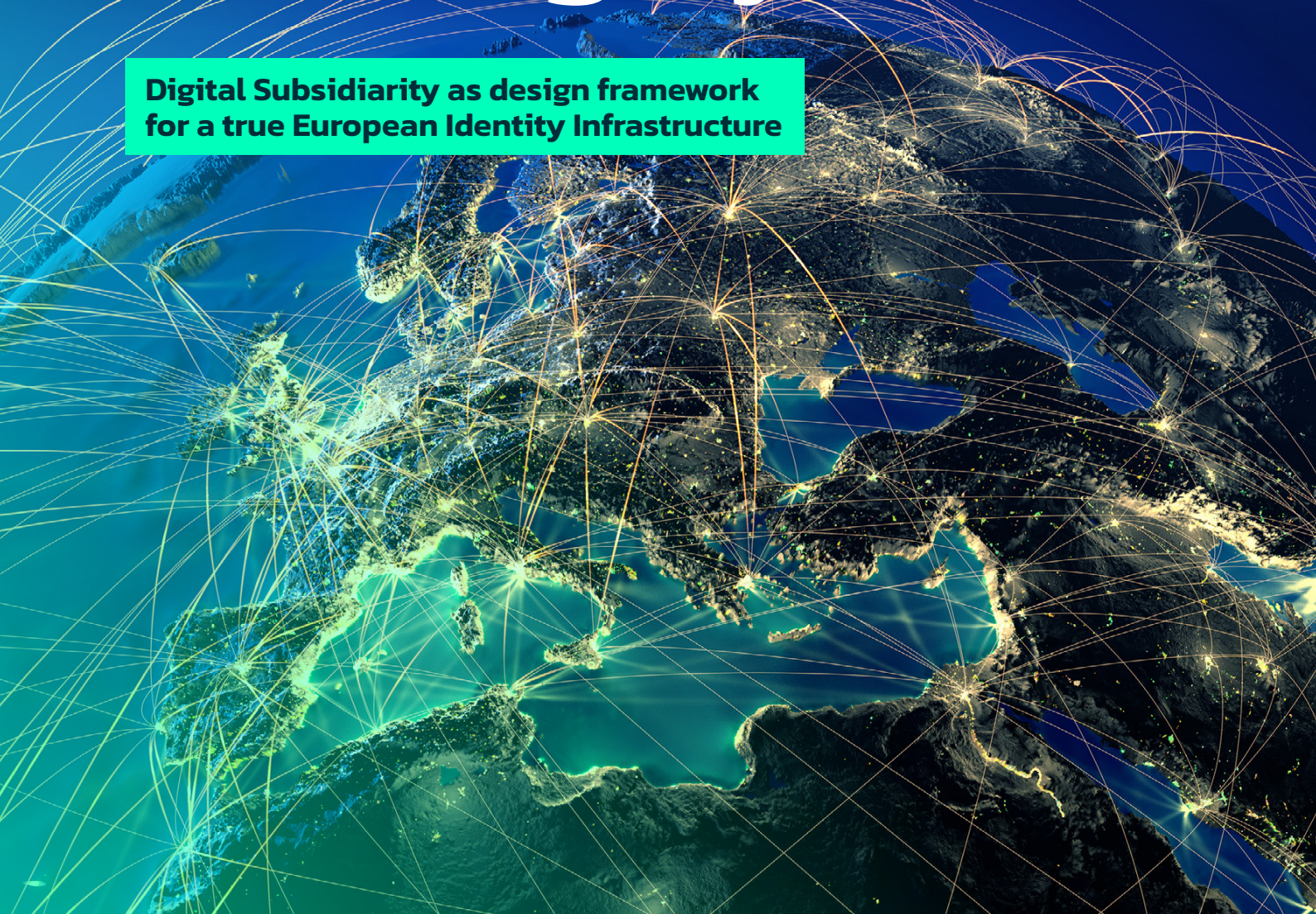
EUROPEAN
DECENTRALISATION INSTITUTE

Digital Identity as the Foundation of European Sovereignty

Digital Subsidiarity as design framework for a true European Identity Infrastructure



May 2026

A publication by the European Decentralisation Institute

00 Executive Summary

Digital sovereignty means that European citizens, organisations, and governments can act independently, predictably, and legitimately in the digital realm. Identity is the first layer of sovereignty: without controlling how you prove who you are, the exercise of every other digital right is contingent on the governance choices of whoever controls the infrastructure.

Europe's digital identity landscape reflects a structural lag: when public and commercial life moved online, public institutions extended identity into the digital realm slowly and partially, while commercial actors moved quickly. The result is that significant portions of citizens' digital lives now depend on commercial identity systems and that public-sector frameworks arrived too late to displace.

The reflex toward centralised state-issued digital identity addresses commercial capture but creates a different concentration of control. Neither model is constitutionally acceptable for Europe.

An alternative path exists, grounded in a principle that European governance already holds: subsidiarity. Applied to digital identity, digital subsidiarity means that credentials sit with citizens, issuance sits with local governments, verification sits with contextually constrained service providers, and only the minimum necessary governance sits at the supranational level. This is not a technical design choice but a constitutional one. In fact, this policy brief illustrates that it is the only arrangement under which digital sovereignty becomes operational rather than rhetorical.

Five Core Findings

1. **Digital identity is not a technical or administrative function**. It is the primary interface between citizens and their rights. Its governance architecture is a constitutional question and a critical element for the digital public infrastructure.
2. The structural problem is not fragmentation but a **missing bridge between physical and digital identity**. As public life moved online, identity was never extended into the digital realm with the constitutional and democratic infrastructure that governs physical identity. The vacuum was filled by commercial actors, producing both visible fragmentation and a deeper structural capture of identity by dominant platforms, predominantly outside European legal reach. The reflex of centralised state identity addresses capture but introduces concentration risks of its own.
3. The EU's eIDAS 2.0, Switzerland's e-ID Act, and the UK's digital identity framework each indicate genuine progress. However, none of them fully resolves **the core governance questions of power, control, and democratic accountability**.
4. Digital subsidiarity, the principle that governance should operate at the most suitable and lowest competent level, provides the organising logic for a European.
5. **Digital identity, digital sovereignty, and digital subsidiarity** are not separate policy tracks. They form a single, interdependent governance architecture.

FOUR POLICY PRIORITIES FOR THE NEXT 36 MONTHS:

1. Enshrine control over digital identity as a **fundamental right**, with non-exclusion protections and delegation mechanisms for vulnerable citizens, applicable and enforceable across the EU, Switzerland, the UK, and ultimately all Council of Europe member states.

2. Mandate **distributed issuance and revocation** through local governments and agencies, with **guaranteed in-person access points** and constitutional rights of recourse, across all European identity frameworks.

3. Build regulatory protection against identity overreach by establishing **unlinkability-by-default** as a binding architectural requirement across all European identity frameworks. Develop **sector-specific Credential Scope Regulations** that define the maximum credential set requestable for each transaction category. Establish a **Digital Identity Ombudsman** function within national data protection authorities, and mandate independent conformance testing on privacy-by-design implementations across the EUDI Wallet, Swiyu, and the UK digital identity framework.

4. Adopt a **Pan-European Identity Trust Framework** grounded in open standards, constitutional change-control mechanisms, mutual recognition, and systems harmonisation. Frame it as a global benchmark, inspired by the *OECD Recommendation on the Governance of Digital Identity*.

01 Identity is at the Center of the Sovereignty Gap

Europe has a sovereignty gap: it excels at writing digital rules, yet much of its backbone runs on non-European, highly centralised infrastructures. This dependency limits Europe's ability to enforce its own norms and to act under stress, creating a sovereignty gap: policy ambition in Brussels depends on systems that Europe neither owns nor can meaningfully steer.

Nowhere is this gap more consequential than with digital identity. Identity is not just another layer of the digital stack, it is the interface between citizens and their institutionally protected and supported rights. Without a functioning digital identity, citizens cannot access welfare, public services, healthcare or financial systems. Organisations and public authorities cannot engage in trusted economic transactions.

> **Identity is the prerequisite for the enjoyment of every other right in the digital age, what Hannah Arendt called the "right to have rights" now rendered digital.**

The root cause

For most of the modern era, identity has been a public good. States issued identity documents under constitutional and administrative frameworks; courts adjudicated disputes; civil registries anchored the legal personhood of citizens; and the rules governing how identity could be requested, verified, and challenged were written into law. Physical identity carried legitimacy because it was governed by accountable institutions.

Digital identity was initially not built as an extension of this framework. As public and commercial life moved online from the late 1990s onward, public institutions extended the constitutional infrastructure of physical identity into the digital realm slowly and partially, while commercial actors moved quickly. In Europe, eIDAS 1.0 in 2014 established cross-border recognition of national eID schemes for public services, but its scope was deliberately narrow and its uptake uneven across Member States. By the time the regulatory framework began to deepen, with eIDAS 2.0, the Swiss e-ID Act, and the UK Digital Identity and Attributes Trust Framework, commercial identity systems had already become structurally embedded in citizens' digital lives. The actors who needed identity to function for their own commercial purposes, platforms, payment providers, telecoms, and the dominant commercial ecosystems whose business models depend on knowing who their users are, had built proprietary identity systems for their own use, and the network effects, integration depth, and data accumulation made these systems difficult to displace. The visible result, a proliferation of incompatible logins, credentials, and wallets, is what is usually called fragmentation. But fragmentation is the symptom, not the cause.

The cause is that the legal and constitutional status of identity has crossed into the digital domain only partially and belatedly, leaving commercial identity systems as the de facto infrastructure for substantial portions of citizens' digital lives. Two consequences follow.

First, **interoperability between physical and digital identity was never established**. The credentials a citizen holds in their physical wallet, government identity documents, professional qualifications, residence permits, do not natively translate into digital form with the same legal weight, and the digital credentials accumulated through commercial relationships do not connect back to the public framework that gives physical identity its democratic legitimacy. The two worlds developed in parallel rather than as extensions of each other.

Second, and as a direct consequence, **identity has been captured by commercial actors that are now structurally embedded in citizens' access to public and private services**. This is not the result of a policy choice that can be reversed at will. A generation of digital infrastructure has been built on commercial identity layers, and the network effects, integration depth, and data accumulation now make exit costly. The capture is most acute in the case of the dominant US platform ecosystems whose wallet, account, and authentication systems serve as the de facto identity layer for substantial portions of digital life across Europe.

The United States illustrates how this happens in the absence of public-sector intervention: no national digital identity system, a 2005 federal floor law (REAL ID) governing physical document standards, a voluntary Mobile Drivers License (mDL) programme with acceptance in 21 States, and an identity access layer that has accordingly been built by Apple, Google, and Samsung. For the US, this carries domestic costs but remains within domestic legal reach. For Europe, importing the same pattern means that the rules governing how citizens prove who they are, including rules that may be modified by foreign executive action or commercial decision, are set outside the legal order of the citizens who rely on them, and a foundational layer of citizenship runs on rules Europe does not write and cannot effectively change.

The reflex toward concentration is also wrong

Where the gap between physical and digital identity has been recognised, the typical reflex has been to close it through centralisation: a single state-issued digital identity, a unified database, a national wallet. This addresses commercial capture but introduces a different structural problem.

India's Aadhaar demonstrates the centralised state-command model at scale: rapid enrolment of virtually the entire adult population, unified infrastructure, and direct welfare delivery, but also citizens locked out of food subsidies through database errors, with no offline fallback and no meaningful appeals route. The Indian Supreme Court had to partially strike down mandatory Aadhaar linkage for welfare schemes. The lesson is not that centralisation is more dangerous than commercial capture, but that both are failure modes of the same underlying problem: control over identity sitting too far from the citizens who depend on it, whether that distance is jurisdictional (foreign commercial actors) or institutional (a central state database insulated from local accountability).

Concentrated identity infrastructure is also a security honeypot. The 2025 IDMerit incident, in which a misconfigured database left approximately one billion KYC records across 26 countries publicly accessible without authentication, demonstrated what catastrophic failure of concentrated identity infrastructure means at population scale. The risk is structural, not incidental.

The European problem, stated correctly

The challenge is that European public-sector frameworks for digital identity –eIDAS, the Swiss e-ID Act, the UK Digital Identity and Attributes Trust Framework– arrived after commercial identity systems had already become structurally embedded in citizens' digital lives, and they do not yet match the constitutional and democratic depth of the framework that governs physical identity. The task is to close that gap, extending the legal weight of physical identity into the digital realm, without simply concentrating control at a level too far removed from citizens.

Two design commitments follow.

Against commercial capture, the rules and infrastructure governing digital identity must sit within European democratic institutions and legal frameworks at every layer, from standards and certification through wallet provision to revocation governance. Identity must be treated as the public good it has historically been in the physical world, even when its operation is technically distributed.

Against state concentration, control must sit at the lowest competent level, close enough to citizens that democratic correction remains possible, with the architecture itself preventing aggregation upward.

These two commitments are not in tension. They are the two dimensions of digital subsidiarity, set out in Section 2.

For Europe, across the EU, Switzerland, the United Kingdom, and all 46 European Council member states, neither continued commercial capture nor concentrated state control is acceptable. The question is whether the governance frameworks now being built across these jurisdictions embed a common design logic capable of bridging the physical-digital identity gap on European terms.

02 Digital Identity, Sovereignty, and Subsidiarity as a Unified Framework

What existing frameworks achieve and what they leave open

The **EU**'s eIDAS 2.0 and the European Digital Identity Wallet establish legally recognised interoperability, privacy protections, and a cross-border framework for electronic identification means and identity attestation. This is substantial progress on the technical and legal interoperability problem. But what it does not fully resolve is the governance of the underlying infrastructure. The regulation constrains who may operate as a wallet provider and mandates open-source architecture, but only for user-facing, frontend components. Additionally, it does not determine who controls the authoritative registers and authentic sources on which credential issuance depends, how those registers will be governed over time, or what constitutional safeguards will apply when the technical architecture is modified through implementing acts rather than primary legislation.

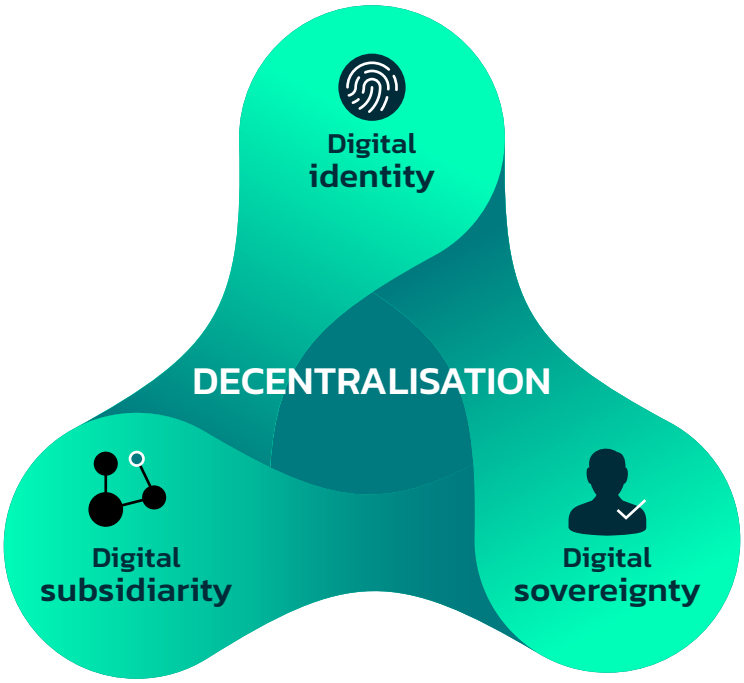
Switzerland's e-ID Act (in force from 2026) and Swiyu infrastructure reflect a strong democratic legitimacy requirement; the 2021 referendum rejection of the previous model was explicitly a rejection of private-sector control over public identity functions. Swiss citizens rejected the privatisation of a fundamental right. The new Swiss approach places issuance firmly in the hands of the federal state while preserving citizen control over credential presentation. It addresses the risk of commercial capture, but opens broader governance questions about central state control, issues that Switzerland's direct democratic mechanisms, including referendums, are designed to manage over time.

The **United Kingdom**'s digital identity framework, built around the Digital Identity and Attributes Trust Framework and the Data (Use and Access) Act 2025, establishes certification and governance mechanisms for a market of certified identity service providers. It addresses fragmentation and provides a legal basis for digital identity across public and private sectors. However, its reliance on a competitive market of providers raises questions about long-term governance stability, the practical exit rights of citizens whose data is held by certified operators, and whether market dynamics over time will lead to concentration among a small number of dominant providers.

Each framework makes genuine progress in its own terms. None of them provides the constitutional governance architecture that subsidiarity-based design requires.

Three concepts, one governance architecture

The strategic opportunity is to treat digital identity governance across Europe not as a set of parallel technical compliance exercises but as a shared constitutional project. Three concepts currently treated as separate policy tracks must be understood as components of a single governance architecture.



Digital identity is the trust infrastructure. It is the mechanism through which citizens, governments, and organisations interact in the digital realm. While traditionally tied to singular events, like a border crossing, identity in the digital realm is about life circumstances over time, linking a person with vital services like healthcare, insurance, and social security. Its architecture determines who holds power and who holds rights in every digital transaction. Technical choices about credential storage, issuance authority, and verification protocols are not neutral: they are governance choices with constitutional implications.

Digital subsidiarity is the governance principle. The subsidiarity principle is already a constitutional requirement of EU governance under Article 5 of the Treaty on European Union, and a foundational value in Swiss federal governance. Digital subsidiarity prescribes that tasks and functions should be performed at the level best fitted to fulfil them, ensuring higher authorities do not usurp functions that can be managed effectively by lower entities, such as local governments, civil society organizations or individuals. . For digital identity, this means that citizens hold their own credentials, issuance sits with local government and verification is constrained to what the context requires. European and national-level governance limited to the minimum scaffolding necessary for interoperability and constitutional compliance. Subsidiarity is not a technical arrangement but a democratic value.

Digital sovereignty is the strategic objective. It means that European citizens, organisations, and governments across the EU, Switzerland, the UK, and the broader European space, can act independently, predictably, and legitimately in the digital realm. Identity is the first layer of sovereignty: without controlling how you prove who you are, the exercise of every other digital right is contingent on the governance choices of whoever controls the infrastructure.

The structural logic connecting all three is the same: over-centralisation in any dimension creates single points of failure, concentrates power in ways that invite capture or misuse, and erodes the distributed accountability that democratic governance requires. To address these risks, digital identity needs to be based on decentralisation as a design requirement

> **Europe cannot achieve digital sovereignty without a digital identity layer, and neither can succeed without digital subsidiarity as the organising design principle**

03 Why Decentralisation is a Design Requirement

Decentralisation is the practical mechanism through which digital subsidiarity becomes operational at the infrastructure level. Without it, governance principles stated in policies remain unenforceable in the systems layer.

First, decentralised control of digital identities empowers the citizen. A citizen who does not hold their own credentials does not, in any meaningful sense, control their identity. The EUDI Wallet, Swiyu, and the UK trust framework all move in this direction. The next step is ensuring that the wallet and credential infrastructure itself is not concentrated in a small number of operators, whether public authorities or private organisations, whose governance falls short of adequate democratic accountability.

Second, a decentralised identity infrastructure avoids single points of failure, thereby ensuring resilience. The 2025 IDMerit incident, in which a misconfigured database left approximately one billion KYC records across 26 countries publicly accessible without authentication, demonstrated what a catastrophic failure of centralised identity infrastructure means at population scale. Distributed architectures eliminate this class of attack surface by design, and they ensure continuity under geopolitical stress: if a foreign infrastructure provider becomes unavailable or hostile, distributed systems continue to function. Centralised ones do not. This is a resilience requirement, not an ideological preference.

Third, decentralisation promotes interoperability that requires open protocols, not proprietary systems. The temptation in any large-scale identity project is to build proprietary infrastructure. Proprietary systems generate vendor lock-in, which is the exact dependency trap that digital sovereignty is designed to escape. Open protocols and open standards are the technical prerequisites for the distributed governance model that subsidiarity requires. Any identity infrastructure receiving European public funds that introduces proprietary lock-in without defined exit rights is, structurally, a risk for digital sovereignty.

Fourth, a decentralised architecture ensures that digital identity infrastructures are democratically accountable. Governance cannot authorise what the architecture cannot enforce. If identity infrastructure cannot be independently audited, if rule changes cannot be tracked and contested, if citizens and data protection authorities cannot verify how the system behaves, then accountability is a policy commitment without a technical basis.

Transparent, auditable, distributed architectures are the precondition for genuine democratic oversight, whether in Brussels, Bern, or London.

> **A sovereign Europe in the digital age will not be built through centralisation, but through distributed trust infrastructures.**

04 Digital Identity through Digital Subsidiarity: Four Functions

Digital subsidiarity requires resisting the notion that identity is a monolith. "One ID to rule them all" is not a European value. Identity is an assemblage of distinct functions, each requiring governance at the appropriate level. Therefore, getting this architecture right is a constituting act.

FUNCTION 1: Attestation and Delegation (Citizen Level)

The most fundamental identity function is enabling citizens to attest to who they are and to delegate this capacity when needed, whether as individual or representing other legal entities like a firm. Digital subsidiarity here means citizens hold their credentials, not governments or platforms. They control access and can delegate granularly and revocably to a caregiver, a legal representative, or a parent acting for a child. This function should be maximally inclusive, enabling citizens with little digital literacy, accessibility issues, and limited access to digital infrastructures.

The principal risk is that monolithic systems are built around the individual as a single, unitary actor. This excludes the elderly, the disabled, and the vulnerable. All three major European frameworks (EUDI Wallet, Swiyu, and the UK trust framework) have work to do on relational identity design. Even the EUDI Wallet ARF's current treatment of delegation and representation is insufficient for the real-world complexity of how people manage their digital lives.

FUNCTION 2: Issuance and Revocation (Local Level)

Issuance and revocation are the democratic backbone of digital identity. Ultimately, democratically accountable governments at the closest level to the citizens hold this mandate. Citizens must be able to walk into their local municipality office or pre-existing public networks, such as post offices, employment centers, and tax offices, to request or challenge their digital identity. Digital identity cannot become a cost-cutting exercise that eliminates local access points.

The risk is centralised issuance without adequate fallback or appeals infrastructure. This is the Aadhaar failure mode, and it can happen again in a European context if implementation choices are made without this constraint in mind. Switzerland's new e-ID model, with cantonal administration as the natural level for in-person services, offers a structural reference. The UK's reliance on certified private providers creates a gap here that the regulatory framework must close. EU Member States' eIDAS 2.0 implementation plans vary considerably in their treatment of local access, implementing regulations should make in-person issuance and revocation pathways a mandatory minimum.

FUNCTION 3: Verification and Access Management (Service Provider Level)

The verification process by which a service provider confirms a citizen's eligibility should be distributed across a plurality of public and private actors. Three distinct constraints must hold simultaneously, and the current frameworks conflate them.

The risk is scope creep: verification becoming profiling. When identity systems permit verifiers to see more than the transaction requires, verification becomes a surveillance mechanism dressed as a compliance function. This risk is present in all three major European frameworks and is not adequately addressed by general data minimisation principles alone. Sector-specific enforcement, with teeth, is required.

Contextual integrity requires that service providers request only the credentials strictly necessary for the specific transaction. A landlord has no legitimate interest in an identity history; an insurance company has no legitimate interest in a citizen's full credential stack.

Data minimisation requires that, within a given credential request, only the minimum attribute is disclosed. Proving age-eligibility for an age-restricted purchase requires a yes-or-no attestation, not a date of birth.

Unlinkability is a separate and stronger requirement, and it is the design commitment that distinguishes a European identity architecture from both commercial-platform models and centralised state models. Unlinkability means that, by default, two distinct verifications cannot be correlated to the same citizen, whether by a single verifier observing repeat interactions, by distinct verifiers colluding or sharing a verification service, or by issuers, registries, or revocation infrastructure functioning as correlation surfaces.

This brief proposes unlinkability as a default requirement of European digital identity infrastructure, with re-linking permissible only through a judicial procedure. Where law enforcement, anti-money-laundering investigation, sanctions enforcement, or similarly grounded public interests require the identification of a citizen across transactions, that re-linking must occur through a defined judicial process subject to due-process safeguards, not through architectural exposure that permits routine correlation. The principle mirrors the long-standing constitutional treatment of communications privacy: communications are private by default, and interception requires a warrant. Identity interactions should be treated the same way. The architecture should make unlinkability the path of least resistance, and re-linking the path that requires explicit legal authorisation.

This commitment has **three architectural implications** that the current frameworks do not adequately resolve.

First, delegation of verification to shared service providers, operationally tempting for smaller relying parties, reintroduces precisely the correlation surfaces that distributed verification is meant to prevent. Where shared verification services are used, they must be designed so that the service provider itself cannot correlate verifications across its customers.

Second, revocation architectures must not function as backdoor correlation infrastructure. Repeated revocation checks can correlate verifiers to issuers or to a central revocation repository. Revocation protocols must be designed so that revocation status can be confirmed without revealing the identity of the verifier or the specific credential being checked.

Third, cryptographic techniques including zero-knowledge proofs, blind signatures, and similar approaches can support unlinkability, but the requirement is architectural and the brief takes no position on specific cryptographic implementations. What matters is that the requirement is stated clearly, that re-linking is permissible only through judicial procedure, and that the architecture is designed to make this default robust against operational shortcuts.

The risk the current frameworks insufficiently address is scope creep: verification becoming profiling. When identity systems permit verifiers to see more than the transaction requires, or to correlate across transactions without judicial authorisation, verification becomes a surveillance mechanism dressed as a compliance function. Sector-specific enforcement, with teeth, is required, alongside architectural requirements that make correlation impossible in the default case rather than merely prohibited by policy.

FUNCTION 4: Architecture Design and Governance (European Level)

The rails of digital identity, i.e., technical standards, interoperability protocols, and governance frameworks are a supranational responsibility. But minimalism is the discipline: the European layer should provide only the scaffolding necessary for the lower levels to function and interoperate. It should not centralise functions that can be performed closer to citizens.

The major risk is the politicisation of the identity architecture. When Europe's age-verification and chat control debates risk turning the identity infrastructure into a surveillance tool, the architectural principle of technological neutrality is under threat. The rails must remain politically neutral and legally sovereign: open standards and no single point of capture or failure11.

Accountability Across the Four Functions

The four-function architecture only operates as a sovereignty instrument if each function carries an enforcement layer. The matrix below specifies, for each function, who should be responsible, who should supervise, who should bear liability, what citizen recourse should exist, what offline or in-person fallback should apply, and what legal instrument should create the duty. It describes the regime this brief recommends, not the regime currently in force. Several of the cells describe duties, liabilities, and instruments that do not yet exist in any of the three European frameworks; those are precisely the gaps the policy priorities in Section 5 are designed to close.

	FUNCTION 1: ATTESTATION & DELEGATION	FUNCTION 2: ISSUANCE & REVOCATION	FUNCTION 3: VERIFICATION	FUNCTION 4: ARCHITECTURE & GOVERNANCE
RESPONSIBLE ACTOR	Citizen (or delegated representative)	Local government or accredited public body	Service provider (relying party)	European Identity Governance Council; standards bodies
SUPERVISORY BODY	National data protection authority; non-discrimination bodies for delegation disputes	National ombudsman; sub-national administrative oversight	Sectoral regulator (financial, health, housing, employment) coordinated with DPA; ENISA for cyber dimension	European Identity Governance Council with standing observers from DPAs, sectoral and cyber supervisors
LIABILITY REGIME	Citizen liable for delegated actions within scope; delegate liable for actions beyond scope	Issuer liable for wrongful issuance, wrongful revocation, and exclusion from local access	Verifier liable for over-collection, unauthorised correlation, and breach of unlinkability default	Governance Council members liable for procedural failures; vendors liable under procurement contracts
CITIZEN RECOURSE	Complaint to DPA; civil action against delegate for misuse	Administrative appeal to local body, escalation to national ombudsman, judicial review	Complaint to Digital Identity Ombudsman; sectoral regulator complaint; judicial action	Standing for civil society and DPAs to delay implementing acts pending review
OFFLINE / IN-PERSON FALLBACK	Paper-based delegation instrument with equivalent legal weight	Mandatory in-person issuance and revocation pathway through local government and public service networks	Non-digital eligibility verification pathway for every regulated transaction category	Public consultation in physical as well as digital form for any architectural change
LEGAL INSTRUMENT CREATING THE DUTY	Digital Identity Non-Exclusion Directive; civil law of agency	eIDAS 2.0 implementing regulation amendment; equivalent national eID law provisions	Sector-specific Credential Scope Regulations; unlinkability-by-default provision in eIDAS 2.0	Pan-European Trust Framework with constitutional change-control mechanism

Read against the current frameworks, the matrix exposes three structural gaps. **Delegation has no clear liability regime** in any of the three European frameworks, leaving caregivers and legal representatives operating in legal ambiguity. **Verifier liability for over-collection or correlation is not consistently established**, because the underlying behavioural standard is not consistently set. And the **legal instruments creating supranational duties today remain implementing acts and procurement guidance rather than primary legislation**, which leaves the entire architecture sitting on a shallow legal foundation. Closing these gaps is the agenda of the policy priorities that follow.

05 Policy Priorities: Four Actions for the Next 36 Months

The following priorities translate digital subsidiarity from principle to operational reality. They build on the foundation laid by eIDAS 2.0 and the EUDI Wallet, while also addressing identity systems in non-EU countries (specifically, the UK and Switzerland).

PRIORITY 1: Enshrine Control over Digital Identity as a Fundamental Right

A citizen-centric digital identity is not a "nice to have." It is the prerequisite for the exercise of every other digital right. Europe must move beyond treating identity as an administrative service or a market function and acknowledge its constitutional status.

Reccomended actions:

1. Adopt a Digital Identity Non-Exclusion Regulation that mandates alternative pathways to vital services for citizens without digital identity access, mirroring the legal protection of cash as a payment method. Digital access to public services should be a right, not a default that excludes those who cannot navigate it. Special assistance should be provided by local governments for citizens with limited digital knowledge and accessibility issues.
2. Establish a minimum humanitarian credential standard, governed by a consortium of Member States and civil society organisations, for vulnerable and displaced persons who cannot access standard issuance pathways. This includes undocumented people, who have an interest in not disclosing their full identity, but who should still enjoy their basic rights. The credential should not be linked to a person's real identity, should be fully privacy preserving, and be available offline (e.g., as a QR code). Introduce delegation rights into the EUDIW ARF, Swiyu, and the UK's digital identity system, enabling citizens to delegate identity attestation to caregivers, legal representatives, or community organisations, with granular and revocable permission scoping. This is absent or inadequately specified in all three current frameworks.
3. Mandate the European Fundamental Rights Agency (FRA) to publish biennial assessments of digital identity exclusion across Member States, with defined remediation obligations. Equivalent monitoring should be established in Switzerland and the United Kingdom.
4. Bring the case to the Steering Committee for Human Rights (CDDH) and the Parliamentary Assembly (PACE) to support the development of new legal standards and instruments, and ultimately promote this right across the 46 Member States of the Council of Europe.

PRIORITY 2: Mandate Distributed Issuance and Revocation

Digital identity must remain accessible through local, physical points of contact. Issuance and revocation should not be fully digitised into systems that require expensive hardware or reliable connectivity. Local government and public services are the right level for this function.

Reccomended actions:

1. Amend eIDAS 2.0 implementing regulations to require that every Member State maintains an accessible, in-person issuance and revocation pathway through local government offices and public services networks, with defined service-level standards. The same should apply to non-EU national eID laws.
2. Launch a co-design programme, structured as a set of funded municipal pilots, in which progressive local authorities and offices partner with the European Commission and civil society to develop distributed issuance models. Publish learnings as open-access governance blueprints.
3. Draw insights and lessons-learnt from Estonia's X-Road architecture to develop a peer-to-peer data-exchange layer that allows local agencies to interconnect securely without routing all interactions through a central node.
4. Establish a Digital Identity Resilience Fund at EU level, with equivalent provisions in Switzerland and the United Kingdom, to support offline-capable identity fallbacks and maintain access for rural, digitally underserved, and border communities.

PRIORITY 3: Build Regulatory Protection Against Identity Overreach

Contextual integrity must become an enforceable legal principle in digital identity interactions. The data minimisation principle in GDPR is the closest existing precedent. Identity regulation must go further, embedding the minimisation-by-design principle sector by sector, making clear what credentials may be requested and under what circumstances.

Reccomended actions:

1. Establish unlinkability-by-default as a binding architectural requirement of European digital identity infrastructure, with re-linking permissible only through a defined judicial procedure subject to due-process safeguards. The principle should be written into eIDAS 2.0 implementing regulations, the Swiss e-ID Act, and the UK Digital Identity and Attributes Trust Framework, and should govern verifier behaviour, revocation infrastructure, and any delegated verification services. Sector-specific Credential Scope Regulations (developed for healthcare, housing, employment, insurance, and financial services) should specify the maximum credential set requestable for each transaction category, operating against the unlinkability-by-default baseline.
2. Establish a Digital Identity Ombudsman function within national data protection authorities, with the power to receive and investigate citizen complaints about identity overreach, and to impose fines comparable to GDPR enforcement.
3. Provide institutional support and regulatory sandboxes for citizen-owned data cooperatives that can serve as non-commercial verification infrastructure, and would strengthen the EU's identity ecosystem vis-a-vis powerful US big tech companies. The EU's Data Governance Act, alongside equivalent provisions in Switzerland and the United Kingdom, already provides a legal basis for this. What is missing is the political will to use it as a genuine alternative to commercial identity providers rather than a theoretical option.

4. Commission an independent conformance testing programme covering privacy-by-design and data minimisation implementations across the EUDI Wallet, Swiyu, and the UK digital identity framework. The programme should be convened through the OECD or the Council of Europe, and public reporting should be a condition of the mandate, not an optional addendum.

PRIORITY 4: Adopt a Pan-European Identity Trust Framework with Constitutional Safeguards

The "rails" of European digital identity need a governance framework that is technically open, politically neutral, and constitutionally robust. The Canadian Pan-Canadian Trust Framework (PCTF) provides a useful reference for federated governance design and its uneven provincial adoption offers a warning about the gap between framework and implementation. The OECD Recommendation on the Governance of Digital Identity likewise calls on adherents to establish national or regional trust frameworks.

Reccomended actions:

1. Commission a multi-stakeholder European Identity Governance Council, comprising EU Member State representatives, Swiss federal and cantonal representatives, UK government representatives, civil society organisations, independent technical experts, and data protection authorities from all participating jurisdictions to develop and maintain a Pan-European Trust Framework.
2. Mandate open standards and technological neutrality as non-negotiable requirements in all identity infrastructure procured with public funds across all three jurisdictions.15 Proprietary lock-in should be prohibited through binding procurement rules, not guidance.
3. Require quantum-resistant cryptography readiness and zero-knowledge proof capability as forward-looking technical requirements in the Trust Framework. NIST post-quantum cryptography standards (FIPS 203, 204, 205) are published. W3C Verifiable Credentials 2.0 is stable. Denmark's national digital identity wallet AltID is deploying ZKP-based selective disclosure at national scale, demonstrating production readiness.
4. The Trust Framework should mandate unlinkability-preserving cryptographic techniques as a baseline capability, including zero-knowledge proof support and unlinkable revocation protocols. NIST post-quantum cryptography standards (FIPS 203, 204, 205) are published. W3C Verifiable Credentials 2.0 is stable. Denmark's national digital identity wallet AltID is deploying ZKP-based selective disclosure at national scale, demonstrating production readiness. The architectural target is not a particular cryptographic primitive but the unlinkability requirement set out in Function 3: re-linking should require judicial authorisation, not be available by default.
5. Establish constitutional change-control mechanisms: any modification to root identity infrastructure in any participating jurisdiction must undergo a transparent, time-limited, multi-stakeholder review process, with standing for data protection authorities to delay implementation pending review. This is the governance safeguard that gives all other protections durability.
6. Instruct the OECD and the Council of Europe to conduct annual Identity Sovereignty Audits measuring the distribution of control across the identity stack, the ratio of open to proprietary components, and the adequacy of fallback mechanisms, across all participating European jurisdictions, not only EU Member States.

7. Mandate that credential issuance operates at the lowest competent authority in every domain. Civic and residency credentials issue from local government; professional and qualification credentials issue from accredited professional bodies; humanitarian and inclusion credentials issue under the two-tier model set out in Priority 1. The Trust Framework should explicitly prohibit centralisation of issuance at national or supranational level for any credential type that can competently be issued closer to the citizen.
8. Establish defined access pathways for both registered and unregistered relying parties. The Trust Framework must not create a regime in which only government-approved verifiers can read credentials from a citizen's wallet, since this would convert the wallet from a citizen-controlled instrument into a state-gatekept channel. Unregistered relying parties should have access under default rules that constrain what they may request and how they may handle the data, with registered status conferring additional capabilities (such as access to higher-assurance credentials) rather than gating access altogether.
9. Mandate an open ecosystem of certified wallet providers in every jurisdiction. Citizens must have meaningful choice among wallet providers, all of which meet a binding minimum certification requirement covering security, accessibility, unlinkability-preservation, and exit rights. Single-wallet models, whether state-issued or designated commercial, should be prohibited at framework level. Citizens must be able to migrate between certified wallets without loss of credentials or service continuity.

06 Conclusion: Digital Identity is the Key to European Sovereignty

The governance choices made in the next 36 months (in eIDAS 2.0 implementing acts, in Swiyu's deployment, in the UK's trust framework development, in the procurement decisions of governments across all 46 Council of Europe Member States) will determine the architecture of European digital identity for a generation. Decisions taken now about who controls the credential infrastructure, how issuance is administered, what verification may request, and how the governance rules of the system can be changed will be difficult and expensive to undo once infrastructure has hardened and vendor relationships have locked in.

Europe possesses something that neither the commercial-driven model nor the centralised state model can offer: a democratic tradition that places citizens at the centre, a constitutional framework that protects fundamental rights, and a federal and multi-state structure that embodies the subsidiarity principle. Digital identity built on digital subsidiarity is how that tradition becomes operational in the digital realm and how Europe demonstrates that an independent European model is possible.

> **Europe does not need a single unified identity system controlled from the centre. It needs distributed and resilient trust infrastructure: identity systems that citizens control, local authorities can administer, and European institutions can oversee without monopolising.**

This applies with equal force in Luxembourg and in Liechtenstein, in Berlin and in Birmingham, in Tallinn and in Zurich.

Identity is not just another layer of the digital stack. It is the first question of digital sovereignty: who controls how you prove who you are, controls who you are in the digital world. Europe must answer that question on its own terms.

Authors:

Dr. Wessel Reijers
Dr. Morshed Mannan
Victoria Citterio-Soelle
Prof. Dr. Dr. h.c. Roman Beck
Alessandro Malventano

Reviewers:

Arno Laeven
Jacob Boersma
Prof. Dr. Patrik Hummel
Pavol Hrina
James Monaghan
Kris Kocic
Prof.Dr. Christoph Kreiterling
Alain Brenzikofer
Christopher Goh
Joeri Toet
Dr. Ignacio Alamillo

Interviews:

Dr. Rolf Rauschenbach (Swiyu e-ID)
Tim Bouma (Pan-Canadian Trust Framework)
Pallavi Sharma (Bhutan NDI)

We thank the following organisations and people for their contributions:
the ENS DAO, the Ethereum Foundation, EY Switzerland, Baroness Manzila Uddin (UK House of Lords), Pramod Varma (India's Aadhaar), Felipe González-Zapata (OECD), Michael Butz (European Signature Dialog), Vasily Suvorov (DIDAS.Swiss), Rémi Colin (Self Protocol), Anand Acharya (Bhutan NDI), Marina Markezic (EEI), Sitara Jabeen (Doctor Without Borders), Eli Guenzburger (University of Lucerne), Mike McCabe (OxBow), Konrad Meijer (EY Zurich).

APPENDIX

Digital Identity

GLOBAL COMPARATIVE ANALYSIS

Governance Models, Sovereignty Architectures, Digital Subsidiarity and Lessons for Europe

Research Companion to Policy Brief:

"Digital Identity as the Foundation of European Sovereignty":

Alessandro Malventano

Analytical Framework

This comparative analysis examines nineteen national and sub-national digital identity systems across three categories: globally leading decentralised implementations, centralised counter-models, and emerging contextual cases. Each case is evaluated against a unified analytical framework derived from the policy brief's core architecture: the three-pillar model of digital identity, digital sovereignty, and digital subsidiarity.

The analysis serves as a research companion to the policy brief "Digital Identity: a crucial building block for a Sovereign Digital Europe" providing empirical grounding for its four policy priorities. Cases are selected for analytical contrast: what works, what fails, under which governance conditions, and with what implications for Europe's independent path.

Evaluation Dimension

Each full-analysis case is assessed across seven dimensions:

DIMENSION	ANALYTICAL FOCUS
Genesis & Legal Foundation	Was the starting point law, technology, politics, or existing infrastructure? Who initiated and governs?
Governance Architecture	How is control distributed across citizens, local government, service providers, and central authorities?
Technical Stack	Standards adherence (W3C DIDs, VCs), blockchain use, open-source components, privacy-by-design.
Subsidiarity Alignment	Does the architecture respect the principle that functions operate at the lowest competent level?
Sovereignty Position	Foreign infrastructure dependencies, vendor lock-in risk, geopolitical vulnerability.
Inclusion & Fallback	Non-digital alternatives, provision for vulnerable groups, delegation mechanisms.
Lessons for Europe	Specific takeaways mapped to the brief's four policy priorities.

Cases are not ranked but placed on a spectrum running from citizen-controlled distributed architectures to state-command centralised models. One analytical caveat is worth stating at the outset: the OECD Recommendation on the Governance of Digital Identity (OECD/LEGAL/0491, 2023) explicitly acknowledges centralised, federated, and decentralised models as all legitimate governance choices, requiring interoperability frameworks rather than convergence on a single architecture. The cases designated here as 'counter-models' are not counter-models on architectural grounds alone, they are counter-models on governance and rights grounds: because of how power is distributed, what accountability mechanisms exist, and whether citizen sovereignty is a design requirement or an afterthought. That distinction matters for analytical precision and should be kept in view throughout.

The European Benchmark: eIDAS 2.0 and the EUDI Wallet

The Normative Achievement

The revised eIDAS Regulation (EU 2024/1183) represents the most comprehensive legislative digital identity framework enacted by any jurisdiction to date. It mandates that all 27 EU Member States provide at least one EU Digital Identity Wallet (EUDIW) to citizens, residents, and businesses by December 2026. Regulated private sectors – banking, healthcare, telecommunications – must accept these wallets by December 2027.

The EUDI Wallet architecture is built around the wallet as a citizen-controlled instrument: users store, manage, and selectively disclose digital credentials, including national identities, professional qualifications, and educational diplomas. Cross-border interoperability and mutual recognition are legal requirements, not technical aspirations.

The broader European landscape is more extensive than the EU mandate alone. Across 43 countries and 215 identity solutions (52 already eIDAS-notified) Europe exhibits deep historical roots in digital identity infrastructure, with several national schemes dating back to 2002–03. Five EU-level large-scale pilots (NOBID, DC4EU, POTENTIAL, EWC, and the new arrivals APTITUDE and WE BUILD) are all wallet-centric public-private partnerships stress-testing the architecture.

What eIDAS 2.0 Resolves and What It Does Not

eIDAS 2.0 definitively resolves EU interoperability and cross-border legal recognition. It establishes a mandatory floor for wallet availability and sectoral acceptance, and it embeds privacy-by-design and selective disclosure as technical requirements. These are genuine constitutional achievements.

However, as the policy brief correctly identifies, eIDAS 2.0 leaves three critical questions only partially answered. First, the power question: who controls authoritative registers and governs credential issuance infrastructure? The regulation mandates wallet availability but does not prescribe distributed issuance architectures. Second, the subsidiarity question: the regulation does not prevent member states from implementing centralised national backends that route all interactions through a single node. Third, the enforcement question: verification scope creep and identity overreach by commercial service providers remain inadequately addressed. A fourth tension has become visible in early implementation: the GDC25 proceedings (Geneva, July 2025) documented that within the EU, member states pursuing very high security levels are generating low inclusion in practice, and that 'one person, one device' architectures are creating barriers for family-assisted e-government scenarios, the elderly, the disabled, and those relying on caregivers. This is not a criticism of eIDAS 2.0 as a legal instrument; it is evidence that the inclusion dimension of Priority 1 is already a live implementation challenge, not a theoretical risk.

The eIDAS Gap

The global cases analysed in this document illuminate precisely the questions eIDAS 2.0 leaves open: governance architecture, subsidiarity at the issuance layer, verification scope enforcement, and the relationship between democratic legitimacy and technical architecture. They do not replace the European framework but stress-test it.

PART I **GLOBAL DECENTRALISED CASES – FULL ANALYSIS**

1. SWITZERLAND: Democratic Legitimacy as Design Brief

Overview

Switzerland's e-ID journey is analytically unique in global digital identity governance: it is the only national identity system to have been rejected by popular referendum, redesigned from the ground up in direct response to that democratic verdict, and then approved by direct democracy in a second vote. This trajectory makes it the most democratically validated identity system in the world, and the most instructive case for the European Union's legitimacy challenge.

Genesis and Legal Foundation

The first Swiss e-ID law, rejected in a March 2021 referendum by 64% of voters, was defeated precisely because it outsourced identity issuance to private companies, with the state in a secondary validation role. Swiss citizens rejected the privatisation of a fundamental right. The lesson was absorbed thoroughly.

The rebuilt framework took the opposite approach. The Federal Act on Electronic Identity Credentials and Other Electronic Proofs of Identity (E-ID Act), passed by the federal parliament on 20 December 2024, places issuance firmly in the hands of the federal state while preserving citizen control over credential presentation. Swiss citizens confirmed this redesign in a referendum on 28 September 2025, approving it by a clear majority.

Architecture: The Swiyu Trust Infrastructure

The Swiyu ecosystem (Switzerland's digital trust infrastructure) is built around a state-issued, citizen-controlled wallet. Key architectural principles:

State issuance: the federal government is the sole issuer of the foundational e-ID credential, eliminating the public-private ambiguity that doomed the first law.

Citizen control: credentials are held in the Swiyu wallet on the citizen's device, not in a central database; citizens control selective disclosure.

Voluntary and free: use of the e-ID is not mandatory and carries no fee; it supplements rather than replaces the physical identity document.

Open source: the Swiyu infrastructure and wallet code are publicly available on GitHub, ensuring auditability and preventing vendor lock-in.

SSI-inspired, not pure SSI: the system draws heavily on self-sovereign identity principles (designed to "ambition level 3") but is not a pure SSI implementation. Privacy is enforced through selective disclosure and device-binding: eID personal data are stored on and bound to a specific device. A change of device requires full re-onboarding and the issuance of a new digital identity. For additional verifiable credentials beyond the eID, qualified issuers determine whether credentials are device-bound or allow backup and recovery.

A public beta has been available since early 2025. Full rollout via the Swiyu Wallet is planned for 1 December 2026, running closely alongside the EU EUDI Wallet deployment timeline.

Unlinkability is the system's primary privacy mechanism. The Federal Council mandated in December 2024 that the eID achieve unlinkability through a batch issuance model of single-use ephemeral credentials: each credential presentation is cryptographically unique and discarded after use, making it impossible to correlate transactions across verifiers. This mechanism is planned for a future release of the trust infrastructure and is not yet in production in the current public beta. The technical standards stack uses SD-JWT VC for verifiable credentials, Decentralised Identifiers (DIDs), OpenID for Verifiable Credential Issuance (OpenID4VCI), and OpenID for Verifiable Presentations (OpenID4VP).

Subsidiarity and Sovereignty Assessment

Switzerland's approach is a partial implementation of digital subsidiarity. Issuance is state-controlled at the federal level, rather than distributed to cantonal authorities, reflecting the Swiss federal preference for uniform national services in this domain. Subsidiarity is applied more strongly at the citizen layer: wallet control is genuinely individual, and the voluntary principle respects citizen agency.

Sovereignty risks are low in governance terms. The open-source infrastructure and domestic governance reduce foreign dependency, and the 2021 defeat specifically blocked the private-sector model that would have introduced the dependency trap the brief identifies. A conceptual distinction introduced by Rolf Rauschenbach at the April 2026 Zurich roundtable is worth retaining here: digital sovereignty is not the same as digital autarchy. Sovereignty means a state possesses the necessary capacity to exercise control and take action in the digital space to fulfil its governmental responsibilities; it does not require technological self-sufficiency. On that definition, Switzerland's approach is coherent: it accepts hardware dependencies on Apple, Google, and Samsung device secure elements while maintaining governance and infrastructure control at the federal level, and is addressing the hardware dependency question through the GDC Council. Whether this distinction resolves the structural sovereignty concern or merely defers it is an open analytical question.

Interoperability Barriers

Switzerland currently faces both technical and regulatory interoperability barriers with the EU that are absent from most comparative assessments of Swiyu. On the technical side, Switzerland's system is built on DIDs, while the EU's EUDIW relies on x.509 certificates, a fundamental incompatibility that requires bridging solutions rather than native interoperability. On the regulatory side, full interoperability with the EU would require a bilateral treaty, which cannot be negotiated until the Swiss e-ID law formally enters into force. As of the time of writing, EU–Switzerland interoperability is a mid-term goal; the preconditions for negotiations are not yet in place. These barriers are directly relevant to Priority 4's Pan-European Trust Framework: Switzerland is a natural participant in that framework, but the path to inclusion involves resolving a technical incompatibility at the credential format layer, not merely a governance alignment exercise.

Lesson for Europe: Priorities 1 & 4

Switzerland demonstrates that democratic legitimacy is not a constraint on digital identity design. The 2021 rejection and 2025 approval together constitute a democratic deliberation process that produced a constitutionally robust architecture. Europe's Pan-European Trust Framework (Priority 4) requires the same quality of democratic legitimacy, not just technical compliance. The voluntariness principle, e-ID as supplement, not replacement, is a direct model for Priority 1's non-exclusion protections. On delegation, Swiyu is partially implemented: parents hold children's eIDs within the legal representative's Swiyu wallet, and guardians manage eIDs for incapacitated adults. However, professional delegation (to lawyers, fiduciaries, or other representatives) is not yet addressed and remains an open governance and technical challenge. The final policy brief explicitly identifies this gap, noting that delegation rights are absent or inadequately specified in the current Swiyu framework.

2. BHUTAN: Decentralised Architecture within a Centralised State

Overview

Bhutan's National Digital Identity (NDI) system is, from a purely technical standpoint, one of the most sophisticated national-scale self-sovereign identity (SSI) implementations in the world. It is the first nation to anchor its national digital identity on the public Ethereum blockchain. Yet it was initiated by royal decree and operates within a centralised governance system. This paradox demonstrates that architectural decentralisation and political subsidiarity are distinct properties that must both be pursued deliberately.

Genesis and Legal Foundation

Bhutan's NDI emerged as a policy-led initiative under the Digital Drukyul Flagship Program, with strong national commitment envisioned and endorsed by His Majesty the King. The legal foundation is the National Digital Identity Act of Bhutan, 2023, which establishes the statutory governance framework, defines issuer and verifier roles, creates trust registries, and provides the framework for cross-border recognition. The starting point was not a void: Bhutan already possessed a robust national civil registration system. The NDI built on this foundational infrastructure while introducing radically new architectural principles.

Governance Architecture: Functional Distribution

As confirmed in Bhutan NDI's primary documentation, control is deliberately distributed across distinct actors for each identity function:

FUNCTION	PRIMARY CONTROLLER	DESCRIPTION
Issuance	Public authorities & approved institutions	Government agencies and authorised organisations issue verifiable credentials: foundational ID, address, banking, employment details.
Verification	Service providers	Public and private entities verify presented Verifiable Credentials to grant access to services.
Control	Citizens	Individuals store credentials in the NDI wallet and control when and with whom credentials are shared.
Access	Citizens	Explicit consent required before any credential is shared for accessing platforms and services.
Delegation	Citizens (where applicable)	Guardianship Wallet model for caregivers, parents, legal representatives. Currently at proof-of-concept stage.
Revocation	Issuers	Credential issuers retain revocation authority. NDI registry contains identifiers only; no personal data.

Technical Stack

- Blockchain anchoring: In October 2025, Bhutan became the first nation to anchor national digital ID on the public Ethereum blockchain (previously Polygon and Hyperledger Indy), cited for immutability, decentralisation, and long-term viability.
- Standards: W3C DID and Verifiable Credentials Data Model (JSON-LD); DIF Presentation Exchange for selective disclosure; Credo TS for Aries-compatible interoperability.
- Privacy: Offline verification without issuer mediation (no 'phone home'). Selective disclosure via DIF Presentation Exchange. ZKP-compatible architecture, not yet in production.
- Open source: Core repositories publicly available (platform, agent-controller, studio, mediator, ethereum-schema-manager).

The Central Tension

The NDI presents a tension that is analytically critical. The technical architecture is genuinely decentralised: citizen-held credentials, distributed issuer-controlled revocation, no central personal data store, public blockchain anchoring. By every technical measure, it aligns with SSI principles.

Yet the governance origin is top-down. There was no democratic deliberation, no referendum, no multi-stakeholder consultation process analogous to Switzerland's. For a small, cohesive nation-state like Bhutan, this may be operationally effective. For Europe – with its diversity of member states, democratic traditions, and constitutional rights frameworks – the governance origin matters as much as the technical architecture. Subsidiarity is a political value, not a technical property. Bhutan's NDI has the second but not the first.

Adoption Dynamics

As of the April 2026 Zurich roundtable, over 450,000 National Digital Identities had been issued (approximately 60% of the population), a significant penetration rate for a system launched in 2021. Bhutan's rollout challenges were primarily practical: public misconceptions about data centralisation (addressed through clear communication about SSI architecture), institutional integration complexity, and digital literacy barriers in rural areas. Adoption accelerated when the system was connected to high-value everyday services: government authentication, financial onboarding, and e-KYC. The mobile-first wallet design was critical. The core lesson, as Bhutan's own documentation states: technology architecture alone does not drive adoption; governance frameworks, institutional coordination, and high-value early use cases are equally critical.

Lesson for Europe: Priorities 2 & 3

Bhutan confirms that SSI architecture is viable at national scale and that offline verification, selective disclosure, and wallet-based citizen control are technically deployable. However, it illustrates that architecture alone does not produce democratic legitimacy or subsidiarity. Europe's distributed issuance model (Priority 2) and regulatory enforcement against overreach (Priority 3) require the governance layer that Bhutan's royal mandate bypasses.

3. CANADA:
Federation as Both Constraint and Model

Overview

Canada's digital identity ecosystem is structurally the most analogous to Europe's governance challenge: a federal constitutional structure that distributes identity authority across multiple autonomous jurisdictions, combined with a shared need for interoperability and mutual recognition. The Pan-Canadian Trust Framework (PCTF) is the primary instrument for resolving this tension – through governance alignment rather than technical centralisation, a model that maps almost directly onto the brief's Priority 4.

Constitutional Architecture: Why Canada Cannot Centralise

In Canada, provinces retain constitutional authority over identity services. Vital statistics registries, driving licences, health cards, and professional credentials are all provincial. The federal government controls passports and immigration. No single national identity authority exists, and creating one would require constitutional reform. Canada's strategy must achieve national interoperability without a national identity provider.Canada's standard-setting reach extends beyond its own borders. The Digital Governance Council standards derived from the PCTF have been picked up by ISO, giving Canada outsized global influence on the technical vocabulary and conformance criteria of digital identity governance. Canada has also been working directly with the EU on mutually recognisable verifiable credentials, a concrete collaboration that positions the PCTF as a live reference point for European framework design, not merely an analogous model to observe from a distance.

The PCTF, developed through a collaborative initiative of federal, provincial, and territorial governments together with industry and public-sector partners, is the response to this constraint. As Tim Bouma's primary documentation confirms, the PCTF does not prescribe technology or mandate a specific platform. It defines atomic identity processes, shared terminology, and conformance criteria that enable mutual recognition across jurisdictions.

PCTF Architecture: Key Characteristics

- Technology neutrality: The framework treats technology as an interchangeable layer. Different provinces can implement different identity solutions as long as they conform to shared governance and assurance standards.
- Federated trust model: Control is distributed across four actors: authoritative registries (public authorities), issuers (public or private), holders (citizens or organisations), and verifiers (service providers). This separates identity authority from credential use.

- Delegation through legal instruments: Delegation (parent for child, guardian for dependent, accountant for corporation) is managed through legally recognised agency relationships, such as powers of attorney or statutory authority, technically represented as relationship records.
- Distributed revocation: Revocation authority resides with issuers, not a central authority. Foundational identity records remain under exclusive public registry control.
- Technology-neutral privacy: ZKP and selective disclosure can be implemented within the framework, but the PCTF deliberately avoids mandating specific cryptographic techniques, leaving implementation choices to participating systems.

British Columbia: Production Implementation

British Columbia's BC Wallet is the PCTF's most advanced production implementation. Built on the province's Digital Trust initiative and governed by FOIPPA (Freedom of Information and Protection of Privacy Act), the BC Wallet is open-source, user-controlled, and privacy- preserving.

It uses W3C VC standards, stores credentials locally, and is governed by explicit consent requirements. BC has shared learnings openly, including public GitHub repositories for the wallet mobile application, and is positioned as a blueprint for other provincial implementations.

Ontario: The Legislative Gap Cautionary Tale

Ontario's experience is among the most instructive cautionary cases in Canadian digital identity governance, and its lessons transfer directly to Europe. Ontario announced its digital identity programme in October 2020, invested approximately CAD 26 million in enabling technologies, and developed an architecture aligned with W3C VCs and DIDs. The Auditor General of Ontario's December 2024 report then confirmed: the programme was placed on hold, pending legislative updates at both provincial and federal levels.

As of 2026, there is no production digital ID wallet in Ontario. The programme has been paused precisely because the legal framework has not kept pace with the technical design. Ontario illustrates what happens when technical ambition runs ahead of legal grounding: resources are expended, momentum is lost, and citizen trust erodes. The brief's emphasis on legal enshrinement (Priority 1) and constitutional safeguards (Priority 4) are directly supported by Ontario's experience.

Lesson for Europe: Priority 4

The PCTF is the closest real-world analogue to the Pan-European Identity Trust Framework proposed in Priority 4. Canada's successes (federated model, technology neutrality, constitutional respect for subsidiarity) and failures (Ontario's legislative paralysis, uneven provincial adoption) both inform Europe's design choices. Importantly, the relationship is active rather than merely comparative: Canada's Digital Governance Council standards have been adopted by ISO, and Canada has been working directly with the EU on mutually recognisable verifiable credentials. Europe has two structural advantages Canada lacks: a binding regulatory instrument in eIDAS 2.0 and a supranational enforcement mechanism. The lesson is to use both, not as centralising tools, but as the scaffold that makes distributed implementations cohere.

4. JAPAN:
Trust Infrastructure as Protocol, Not Database

Overview

Japan's Trusted Web initiative is one of the most conceptually sophisticated digital identity frameworks in the world, and one of the least understood outside Asia. It is not primarily an identity system in the conventional sense: it is a governance and trust architecture designed to decentralise the internet's trust layer itself, enabling verification of identity and data authenticity without depending on a small number of centralised platforms, whether state or commercial.

Policy Context: From My Number to Trusted Web

Japan's pre-existing identity infrastructure, My Number (2015), is a centralised government-issued twelve-digit identifier linked to tax, social security, and public administration. It has faced persistent adoption resistance rooted in cultural privacy concerns and distrust of centralised data aggregation. The Trusted Web represents the government's strategic response: a commitment to decentralised trust infrastructure as the long-term trajectory, developed by the Digital Agency (created 2021) under the Basic Act on Forming a Digital Society.

Architecture: The Third Way

Japan's architects explicitly reject both the US market-driven model (governance vacuum filled by Big Tech) and heavily centralised models. The Trusted Web White Paper 3.0 defines the framework around three principles:

- Trustless verification: Entities should be able to verify identity and data authenticity without depending on a trusted third party or centralised identity provider.
- Data sovereignty: Individuals and organisations control their own data and can verify the integrity of data they receive.
- Data Free Flow with Trust (DFFT): Privacy, security, and intellectual property protection are not constraints on data flows, but conditions for them, a principle now institutionalised as an Institutional Arrangement for Partnership (IAP) hosted at the OECD.

Technically, the Trusted Web relies on Verifiable Credentials and Decentralized Identifiers. The White Paper specifically highlights Privacy-Enhancing Technologies (PETs), including Multi-Party Computation (MPC), as the mechanism for moving away from centralised identity providers. The DVCC Consortium, formed in 2023 by major Japanese industrial players including MUFG, Fujitsu, and NTT Data, drives industry implementation, with Partisia (a Danish MPC specialist) serving as a key technical partner for real-world pilots.

Geopolitical Dimension: EU-Japan Alignment

The EU-Japan Memorandum of Cooperation on Digital Identities and Trust Services establishes a framework for mutual recognition and alignment of DID standards between the Trusted Web and eIDAS 2.0, making Japan the first non-European country to formally align its

identity architecture with the European framework. This is directly relevant for Europe's foreign policy dimension of digital sovereignty.

The DFFT principle is Japan's diplomatic instrument for projecting democratic, privacy-respecting data governance norms internationally, positioning itself alongside other jurisdictions committed to open and accountable digital infrastructure. Japan's Digital Agency has also explicitly positioned its Trusted Web as compatible with the EU and Canadian frameworks (as noted in the White Paper's comparative governance section).

The My Number Tension

The Trusted Web's ambition sits in tension with My Number's ongoing role as the operational identity infrastructure. Japan's experience with My Number adoption resistance, attributable to persistent public concerns about data aggregation, illustrates the policy brief's warning: centralised identity creates trust deficits that are difficult to reverse. The multi-decade transition from My Number to a Trusted Web-compatible architecture is Japan's version of the governance investment the brief argues Europe must make now.

Lesson for Europe: Priority 4 (Geopolitical)

Japan demonstrates that digital identity governance is a geopolitical instrument, not just an administrative function. The EU-Japan MoC shows that a European identity architecture built on open standards and democratic values can anchor a broader coalition of like-minded governance models. Europe's Pan-European Trust Framework should be designed with global alignment potential - not as a closed system but as an exportable governance model, consistent with the DFFT principle.

5. SOUTH KOREA: Public-Private Scale and the Sandbox Innovation Model

Overview

South Korea completed the rollout of a national Mobile Resident Registration Card to all 52 million citizens in March 2025, making it one of the few countries to achieve full-population national digital identity deployment at speed. Its model combines state-mandated national mobile ID with robust private-sector participation, a regulatory sandbox model for sub-national innovation, and notable international interoperability achievements. It also presents significant cautionary dimensions on scope creep and privacy that are directly relevant to the European analysis.

Governance Architecture

The Electronic Government Act (revised July 2025) provides the primary legislative basis. The Ministry of the Interior and Safety (MOIS) Digital Government Bureau holds central oversight, while the Korea Internet & Security Agency (KISA) serves as the technical auditor for all DID projects, publishing whitepapers and setting security standards for Korea's DID ecosystem (K-DID). This is a federated model with strong central standards: the state defines security and trust criteria while private actors compete in the implementation layer.

The OECD's 2025 Digital Government Review of Korea confirms this as a "federated, digital-authentication platform that allows citizens to use their choice of certified and secure, private, authentication solutions." The Mobile Resident Registration Card holds the same legal validity as a physical ID card and is accepted across public administration, financial institutions, and healthcare.

Private Sector Achievement

Two private-sector stories are particularly instructive. Hopae's COOV wallet, a government-adopted, privacy-preserving digital credential system built on decentralised architecture, served over 43 million users during the COVID-19 pandemic, demonstrating that user-centric design and immediate utility can drive adoption at extraordinary speed. COOV achieved interoperability with the EU and Singapore, making it one of the first private-sector identity wallets to demonstrate practical cross-border credential exchange at scale.

Samsung's integration of the national mobile ID into Samsung Wallet (with plans for international expansion) illustrates both the opportunity and risk of Big Tech involvement. Device-level integration provides convenience and scale; it also creates dependency on a single hardware ecosystem, raising vendor lock-in concerns analogous to the Apple/Google risk in the US context.

The Busan Sandbox

The Busan Metropolitan City's Blockchain Regulation-Free Special Zone is a distinctive governance innovation: a city-level legal sandbox that permits the city to bypass national laws (including the Personal Information Protection Act) in a controlled environment to test advanced data sovereignty models. The B Pass app integrates citizen IDs, library cards, and visitor passes using the Metadium DID public blockchain protocol, enabling rapid experimentation that the national legal framework would otherwise prevent.

This is directly analogous to the municipal pilot model proposed in Priority 2 of the policy brief. One caveat is significant: Metadium Technology Inc. is headquartered in the Cayman Islands, illustrating exactly the sovereignty dependency that Priority 4's procurement rules are designed to prevent.

Critical Limitations

South Korea's model faces documented criticisms that transfer directly to the European analysis. On privacy: the architecture enables persistent behavioural profiling through its authentication model, and the government's approach to age assurance has raised documented concerns about surveillance-by-design. On interoperability: as of mid-2025, South Korea's national digital ID has been assessed as non-compliant with international standards in certain dimensions, creating barriers to the cross-border recognition that COOV's success had suggested was achievable. These critiques validate precisely the contextual integrity enforcement the brief proposes in Priority 3.

Lesson for Europe: Priorities 2 & 3

South Korea demonstrates that rapid national-scale rollout is achievable with public-private cooperation and clear government mandate. It simultaneously demonstrates that without robust contextual integrity enforcement (Priority 3), speed and scale produce surveillance risks. The Busan sandbox is a direct operational model for Priority 2's municipal pilot programme – but the Metadium sovereignty dependency illustrates why Priority 4's procurement rules banning vendor lock-in are non-negotiable.

6. AUSTRALIA:
Voluntariness, Multi-Provider Design, and the Honeypot Solution

Overview

Australia's Australian Government Digital ID System (AGDIS) and its consumer-facing myID application represent the most comprehensively legislated federated multi-provider digital identity system outside Europe. The Digital ID Act 2024 transforms a previously voluntary framework into a legislated national system, establishing architecture, governance, and privacy safeguards that directly parallel the policy brief's four priorities – in several cases providing enacted examples of what the brief proposes.

Legislative Architecture: Dual Regulator Model

The Digital ID Act 2024 is notable for several structural choices that directly mirror the brief's priorities. Parts 4 and 5 establish a dual-regulator model that addresses both market and rights dimensions simultaneously:

- The ACCC (Competition and Consumer Commission): accredits identity providers and ensures the system remains competitive and non-discriminatory. This is the backstop against commercial monopoly.
- The OAIC (Office of the Australian Information Commissioner): provides additional privacy safeguards beyond the standard Privacy Act 1988, specifically for Digital ID. This is the citizen rights backstop against overreach.

This dual-regulator architecture is the closest operational example to the Digital Identity Ombudsman function proposed in Priority 3 of the policy brief.

Why Multi-Provider over Monolithic: The Documented Rationale

The Impact Analysis document justifying the AGDIS legislation explicitly contrasts the federated multi-provider model against a centralised single-database approach across five documented dimensions:

- Honeypot prevention: Decentralisation ensures no single entity holds all citizen identity attributes, reducing the impact of any breach, consistent with the policy brief's ODIDO analysis.
- User choice: Preventing a 'single government identifier' ensures citizens can choose their preferred provider.
- Interoperability: Enabling Digital ID reuse across state, federal, and private sectors, eliminating the documented AUD 3 billion+ in annual economic friction created by fragmented silos.
- Market competition: Allowing private-sector providers (banks, post offices) to compete, fostering innovation rather than a state-run monopoly.
- Hub-and-spoke architecture (IDX): The Identity Exchange acts as a router between providers and services, not a data storage centre, thereby enforcing the principle that no central node holds comprehensive citizen data.

The Voluntariness Principle

Clause 74 of the Digital ID Bill (the Voluntariness Principle) requires that agencies provide a non-digital alternative for every service that uses digital ID. This is the legislative implementation of the brief's proposed Digital Identity Non-Exclusion Directive in Priority 1. Australia has enacted in law what the brief proposes as a European priority.

Current Limitations

AGDIS is primarily a government-services authentication system, not yet a full digital credential ecosystem with portable citizen-held verifiable credentials in the EUDI Wallet sense. The myID application enables authentication but does not yet deliver the full wallet-based selective disclosure model. Australia is at an earlier stage of the transition from federated authentication to distributed credential infrastructure, making its governance achievements more instructive than its technical maturity.

Lesson for Europe: Priorities 1 & 3

Australia's voluntariness principle (legislated non-digital fallback) and dual-regulator model (competition + privacy) provide directly transferable institutional designs for Priorities 1 and 3. The AGDIS impact analysis provides the economic language for justifying federated over centralised architecture. The honeypot prevention rationale is directly applicable to Europe's ODIDO-style breach risk analysis.

PART II **COUNTER-MODELS: CENTRALISED AND MARKET-DOMINATED PARADIGMS**

7. INDIA: The Centralised State-Command Model at Scale

Overview

India's Aadhaar system is the world's largest digital identity infrastructure: a foundational biometric ID linked to a central database serving over 1.4 billion people, with adult enrolment exceeding 97%. It demonstrates what the policy brief characterises as the first dead-end mode, the centralised state-command approach, at the most extreme scale yet attempted. Its achievements and its failures both carry direct lessons for Europe.

Architecture: Foundational Biometric Model

Aadhaar is built on the foundational identity model: a single biometric identifier (iris, fingerprint, and photograph linked to a twelve-digit unique identifier) serves as the root for all government and private sector services. The Unique Identification Authority of India (UIDAI) maintains the central biometric database. Every identity verification in the ecosystem involves, directly or indirectly, a query against or derivation from this central store.

The scale and speed of rollout are genuinely extraordinary. It enabled direct benefit transfer programmes that bypassed corrupt intermediaries, reduced welfare leakage, and extended financial inclusion. These achievements are real and should not be dismissed. The analytical question is not whether Aadhaar functions at scale but whether the failure modes it has generated are compatible with fundamental rights standards.Aadhaar also incorporates a set of privacy-by-design features that are frequently absent from critical assessments. Audit logging is minimal by design: no purpose or location is captured at the point of authentication, and all audit data is deleted after six months by law. A Virtual ID system provides a fungible alias for the permanent UID, allowing authentication without exposure of the underlying identifier. Automatic tokenisation ensures that agency databases store only an agency-specific token rather than the UID itself, limiting the capacity for cross-agency data aggregation. Offline authentication channels exist, via paper, mobile, and W3C Verifiable Credentials, though the offline and online channels do not interoperate. These features represent deliberate design choices that complicate any simple characterisation of Aadhaar as an unreconstructed surveillance architecture. The structural risks identified below are real; they coexist with genuine privacy engineering.

The Structural Failures

Three structural failures are documented and directly relevant to the European analysis:

- Welfare exclusion through biometric failure: Database errors and biometric recognition failures have locked vulnerable citizens out of food subsidies and welfare payments. The Indian Supreme Court was required to partially strike down mandatory Aadhaar linkage for welfare schemes precisely because the exclusion rate was generating constitutional violations of the right to life.
- Limited offline interoperability: while Aadhaar supports offline authentication channels (paper, mobile, and W3C VC), these channels do not interoperate with the online system. In areas with poor connectivity, typically including the most vulnerable communities, citizens are dependent on offline modes that function independently but cannot substitute fully for online verification in contexts that require it. The absence of a unified offline–online fallback pathway remains a design gap.
- Structural overreach potential: The centralised architecture creates the structural conditions for surveillance at scale. The Supreme Court's 2018 Puttaswamy judgment recognised privacy as a fundamental right and limited Aadhaar's mandatory scope, but the structural capability for mass surveillance remains embedded in the architecture.

Counter-Model Lesson

Aadhaar demonstrates the "centralised state-command model" at significant scale. The cases support the policy direction towards distributed issuance with offline fallback (Priority 2), contextual verification enforcement (Priority 3), and constitutional change-control mechanisms (Priority 4). The specific failure mode – biometric exclusion of welfare recipients with no appeals route – is precisely the scenario Priority 1's Digital Identity Non-Exclusion Directive is designed to prevent.

8. CHINA:
State Surveillance Infrastructure

Overview

China's National Digital Identity Framework, operated under the Ministry of Public Security, represents the most extensive integration of digital identity with state-administered behavioural data infrastructure among the cases examined in this analysis. It is architecturally relevant to the European analysis primarily as a contrasting paradigm, illustrating the governance outcomes that arise when citizen sovereignty and democratic accountability are not design constraints – and as a benchmark for understanding where the line between legitimate governance and democratic overreach lies.

Architecture

China's system links a national digital identity (governed by real-name registration requirements) with a comprehensive social and behavioural data infrastructure. It operates under real-name registration mandates for all major digital services and is architecturally integrated with the social credit system – a distributed, multi-agency scoring infrastructure that uses identity linkage to regulate citizens' access to services, travel, financial products, and economic participation.

Recent developments include advances in a 'Real DID' framework, a national digital identity credential infrastructure that uses some of the same technical primitives (DIDs, VCs) as decentralised systems, but within a governance architecture that inverts their purpose. Instead of enabling citizen sovereignty over identity, they enable state surveillance with the appearance of technical modernity. This is a crucial lesson: technical primitives are not intrinsically rights-preserving.

Counter-Model Lesson

China demonstrates that technical infrastructure described as "decentralised" (DIDs, VCs) can be deployed within a governance architecture that does not produce citizen sovereignty as conventionally understood in democratic governance contexts. Constitutional safeguards, not only technical standards, are the mechanism for addressing this risk. The change-control mechanisms and data protection authority veto rights proposed in Priority 4 represent the relevant institutional framework.

9. UNITED STATES:
The Market-Vacuum Model

Overview

The United States does not have a national digital identity system. It has a fragmented patchwork of state-issued licences, a 2005 federal floor law (REAL ID) governing physical document standards, a voluntary programme for mobile driver's licences (mDLs) with acceptance in 21 states, and a de facto digital identity layer dominated by Apple, Google, and Samsung wallet ecosystems. This is the market-vacuum model the policy brief identifies as the second dead-end: not a failed state-command approach, but an absent state creating a governance vacuum filled by commercial actors..

Architecture: The Patchwork in Practice

The US digital identity landscape operates across three tiers. The federal floor is the REAL ID Act (2005), an outdated law governing minimum standards for physical IDs, primarily driven by post-9/11 security concerns. The state layer is where digital identity actually operates: each state issues its own mDL where it has one, governed by state-level legislation with variable privacy and security standards (21 states now have TSA-accepted mDLs as of 2026). The commercial layer is where most private-sector identity interactions happen: Apple ID, Google Account, and Facebook Login function as the de facto digital identity infrastructure for non-government services. This dynamic has a documented history: the OECD's G20 Collection (2021) traced how, in the absence of a federal digital identity strategy, large platforms became 'de facto identity access layers', a process that was already well advanced by 2021 and has deepened since. In the absence of a national framework, the governance space was occupied by commercial actors.

The federal government's primary digital identity product, Login.gov, serves as a single sign-on for federal services but has faced documented criticism for reliance on LexisNexis, a commercial data broker that aggregates vast arrays of personal records from internet sources for identity proofing. This extractive model is fundamentally incompatible with GDPR's Privacy by Design and data minimisation requirements, and illustrates how even government-operated systems in the market-vacuum model inherit commercial data exploitation norms.

The Utah Anomaly

Utah's SB 275 (February 2026) is the most interesting recent US development. The law uniquely defines identity as something inherent to a person and endorsed by the state rather than bestowed by the state, a philosophical shift that moves one US jurisdiction closer to the European rights-based conception of identity. It is a state-level exception that illustrates what a rights-based approach within the US constitutional framework might look like, but it remains isolated and without federal implications.

Three Reasons the US Model Fails Europe

- Commercial shadow identification: Data broker-dependent identity proofing treats identity as a commercial resource, violating Privacy by Design and data minimisation at the root of the system.
- Horizontal interoperability failure: A digital ID accepted at TSA checkpoints may not work at a local bank or across state lines. eIDAS 2.0's cross-border legal recognition mandate has no US equivalent.
- Corporate sovereignty risk: Apple and Google's wallet dominance creates vendor lock-in where citizen identity access depends on hardware ecosystem choice, raising the same structural dependency concerns that European digital sovereignty policy seeks to address.

Counter-Model Lesson

The US model demonstrates that the absence of a rights-based national digital identity framework does not produce a neutral vacuum – it produces a governance space that commercial actors fill on their own terms. Europe's eIDAS 2.0 exists partly because European policymakers observed this dynamic and chose to prevent it. Priority 4's procurement rules against proprietary lock-in, and Priority 3's sectoral credential scope regulations, are the operational responses.

PART III **EMERGING CASES: ADDITIONAL REFERENCE POINTS**

10. EMERGING CASES

The following cases are included as contextual reference points rather than full analyses. Each illustrates a specific dimension of the global landscape that enriches the comparative picture without requiring the depth of treatment reserved for the primary cases.

United Kingdom: GOV.UK One Login

Post-Brexit, the UK has developed its own digital identity trust framework (Gamma 0.4, December 2025), operated by the Office for Digital Identities and Attributes (OfDIA) under the Department for Science, Innovation and Technology. GOV.UK One Login has onboarded over 50 government services and 6 million users. The framework explicitly aligns with four international standards: the Pan-Canadian Trust Framework, eIDAS, NIST 800-63, and ISO/IEC 29115 – making it the most internationally standards-convergent framework outside the EU. The government is moving toward mandating digital ID for right-to-work verification.

A February 2026 survey of 39 digital verification service providers found that 79% cited regulatory diversity as a barrier to international operations, and 62% called for cross-border political or regulatory agreement. These findings validate the brief's argument for a Pan-European Trust Framework: even the UK, with a mature framework and significant deployment, faces the interoperability barrier that common standards are designed to eliminate. The UK's trajectory also illustrates how quickly frameworks can be used for mandatory purposes once deployed voluntarily.

United Arab Emirates: UAE Pass

UAE Pass is a highly integrated, government-led digital identity system providing seamless authentication across government and private sector services. It is technically efficient and widely adopted. However, it operates within a governance context that does not include democratic accountability, separation of powers, or fundamental rights protection in the European sense. Its relevance for the European analysis is as an illustration of what operational efficiency looks like when citizen sovereignty is not a primary design consideration, which illustrates why efficiency alone is an insufficient design criterion for democratic polities.

Ethiopia: Fayda ID

Fayda is Ethiopia's national foundational ID, modelled closely on India's Aadhaar but implemented through the open-source MOSIP framework. Authorised by the Ethiopian Digital Identification Proclamation No. 1284/2023 and administered by the National ID Program (NIDP) under the Prime Minister's office, Fayda issues a unique 12-digit identifier to residents linked to biometric enrolment (fingerprint, iris, face). The programme targets 90 million registered Ethiopians by 2030, supported by World Bank funding. Like Aadhaar, Fayda demonstrates the inclusion-by-design ambition of foundational ID, and shares Aadhaar's structural risks: biometric exclusion potential, no decentralised fallback, and the concentration of identity authority in a single state apparatus.

Singapore: Singpass

Singpass provides a highly integrated authentication layer between government and private sectors, with high adoption and strong user experience. Its primary relevance for European analysis is as a warning about 'phone home' architecture: Singpass's design requires the identity provider to be involved in most verification transactions, enabling persistent logging of where, when, and how often citizens interact with services. This produces behavioural profiling capability that contradicts European values of unlinkability and informational self-determination. Singpass is efficient; it is not subsidiarity-compliant. It is the operational illustration of the verification-shading-into-surveillance risk the brief describes in Section 3.

Brazil: GOV.BR

Brazil's gov.br platform is a single-portal model consolidating all civic interaction into a unified federal platform linked to the National ID Card (CIN) and the CPF tax identifier. Authorised by Federal Law 14.129/2021 and operating as a centralised public system with hundreds of millions of accounts and wide service integration, gov.br demonstrates that centralised digital government can achieve significant scale and service quality. It does not, however, provide citizen-controlled credential infrastructure, selective disclosure, or the distributed issuance model the brief advocates. It is a well-executed administrative efficiency tool that does not aspire to be a sovereignty architecture.

New Zealand: Values-Based Framework

New Zealand's Digital Identity Services Trust Framework, finalised in late 2024, is notable as a values-based approach to digital identity governance. It explicitly foregrounds dignity, inclusion, and equity as structural design criteria alongside technical interoperability - not as aspirational statements but as evaluative requirements built into the framework's conformance criteria. Worth monitoring as a model for how constitutional values commitments can be embedded structurally into a trust framework rather than appended as policy rhetoric.

ANALYTICAL SYNTHESIS:
Mapping to the Policy Brief's Four Priorities

The comparative evidence assembled in this analysis supports and enriches the policy brief's four-priority framework. The following synthesis maps key findings from the cases to each priority.

PRIORITY 1 Enshrine Digital Identity as a Fundamental Right

Evidence from Aadhaar (welfare exclusion through biometric failure, Supreme Court intervention), Australia (voluntariness principle legislated in Digital ID Act 2024, Clause 74), and Switzerland (2021 referendum defeat of private-sector issuance model) collectively establish that treating identity as an administrative function rather than a constitutional right produces both technical failures and democratic legitimacy deficits. Australia's Clause 74 is the closest real-world implementation of the brief's proposed Digital Identity Non-Exclusion Directive. Bhutan's guardianship wallet model and Canada's legally recognised delegation relationships provide operational templates for the delegation rights dimension, a dimension that is acquiring new urgency beyond the human case: GDC25 (Geneva, July 2025) identified the convergence of agentic AI and digital identity as an emerging frontier, noting that AI agents acting on behalf of users will require robust delegation and representation mechanisms that are currently underspecified in every framework examined. Ethiopia and India together define the failure scenario that non-exclusion protections are designed to prevent.

PRIORITY 2 Mandate Distributed Issuance and Revocation

The comparative evidence strongly validates distributed issuance. Canada's federated model demonstrates that multiple issuance authorities within a shared trust framework produce more resilient and legitimate systems than centralised alternatives. Bhutan's functional distribution table shows that separating issuance authority from citizen credential control is technically implemented and operationally viable at national scale. South Korea's Busan sandbox provides a direct operational model for the municipal pilot programme the brief proposes. Australia's hub-and-spoke IDX architecture demonstrates technically how a federated model prevents the central data honeypot problem. Estonia's X-Road architecture, referenced in the brief, is reinforced by the PCTF's peer-to-peer data exchange principles and Japan's Trusted Web's protocol-layer approach.

PRIORITY 3 Build Regulatory Protection Against Identity Overreach

South Korea's documented scope creep problems (behavioural profiling through authentication logging and age verification overreach) provide the negative case for why contextual integrity enforcement is essential at the regulatory layer, not merely the technical layer. Australia's dual-regulator model (ACCC for competition, OAIC for privacy) provides a viable institutional template for the Digital Identity Ombudsman function the brief proposes. Singapore's phone-home architecture illustrates precisely the 'verification shading into profiling' risk the brief describes in Section 3. Canada's PCTF principle of separating identity authority from credential use is the governance mechanism for preventing this. China's 'Real DID' development demonstrates that even technically decentralised credential systems can be co-opted for surveillance purposes without strong regulatory enforcement.

PRIORITY 4 Pan-European Identity Trust Framework

The strongest comparative evidence for Priority 4 comes from five cases. **1.** Canada's PCTF demonstrates that federated trust frameworks can achieve interoperability without centralisation, and that uneven adoption without binding legal requirements (Ontario) undermines even a well-designed framework. **2.** The EU-Japan Memorandum of Cooperation demonstrates that a European identity trust framework built on open standards can serve as an exportable geopolitical governance model, attracting like-minded systems into alignment. **3.** Switzerland's 2021 referendum defeat demonstrates that the constitutional safeguards the brief proposes, multi-stakeholder review, data protection authority veto rights, change-control mechanisms, are not bureaucratic obstacles but the source of democratic legitimacy. **4.** Australia's procurement rationale against proprietary lock-in, documented in its Impact Analysis, provides economic language for the brief's binding procurement rules. **5.** The UK's post-framework interoperability survey (62% of providers calling for cross-border agreement) quantifies the governance dimension of the problem.

Finally, the OECD's G7 Mapping Exercise (October 2024) provides the technical dimension: as of that baseline, no international standards were shared across all G7 members, and only six were shared between any two, meaning the surface-level policy alignment between major digital identity jurisdictions sits on top of deep technical fragmentation. That finding is from 2024; given the pace of development since, the picture may have shifted, but it establishes the scale of harmonisation work that a Pan-European Trust Framework must be designed to address, not assume away.

CONCLUSION:
The European Way Is Validated

The comparative landscape examined in **this analysis confirms three foundational claims** of the policy brief.

First, the two dead-ends are empirically demonstrated. India's Aadhaar shows the centralised state-command model producing systemic exclusion and democratic risk at scale; the Indian Supreme Court's intervention is the institutional proof. The United States shows the market-vacuum model producing commercial capture of identity governance with no democratic accountability; Login.gov's LexisNexis dependency is the operational proof. Both failures are documented, ongoing, and transferable warnings.

Second, the European independent path is not hypothetical. Switzerland, Bhutan, Canada (BC Wallet), Japan, and Australia all demonstrate functional elements of the distributed, citizen-controlled, standards-based architecture the brief proposes. None has yet fully implemented the complete model – but together they constitute the empirical foundation for it. The technical primitives (W3C DIDs, Verifiable Credentials, selective disclosure, open-source wallet infrastructure) are mature, tested, and available. The architecture is feasible.

Third, and most critically, the hardest work is governance, not technology. Ontario is stalled not because the technology is unavailable but because the legislation is incomplete. Bhutan's SSI architecture does not automatically produce subsidiarity because subsidiarity is a political value, not a technical property. Switzerland's 2025 success over 2021's failure reflects a redesign of governance, not of cryptography. South Korea's speed without adequate privacy regulation produced surveillance risk, not sovereignty. This is not a new observation: the OECD's G20 Collection (2021) found that countries with clear governance leadership, defined responsibilities, and legal frameworks consistently outperformed those with strong technology but weak governance, a finding from four years ago that every case in this analysis confirms. The technology stack for European digital identity is mature. Governance choices are what remain to be made.

Europe's democratic tradition, constitutional framework, federal structure, and binding supranational regulatory capacity constitute the governance infrastructure that could transform available technical primitives into a rights-grounded identity system. The comparative evidence does not suggest that Europe must move faster. It suggests that Europe must move with the clarity that governance architecture is a constitutional act – and treat it with constitutional seriousness.

Final Synthesis

Digital identity built on digital subsidiarity is not a position unique to the European context; it represents a convergent direction of travel for every democratic governance system grappling seriously with this challenge. The question Europe must answer is not whether this model is viable. The comparative evidence confirms it is. The question is whether Europe will build the governance infrastructure that makes the architecture real, durable, and democratically legitimate. The choices made in the next 36 months will determine the answer.

Sources and references

Sources are organised by category. Within each category, entries are listed alphabetically by author or issuing institution. URLs were verified as accessible at time of citation. Legislative instruments are cited by official title and enactment date. Interview sources are cited in accordance with standard social science practice for primary qualitative data.

I. PRIMARY SOURCES: INTERVIEWS AND FIELDWORK

All interviews were conducted as part of the research programme for the EDI Policy Brief on Digital Identity and European Sovereignty. Transcripts and questionnaire responses are held by the European Decentralisation Institute.

European Decentralisation Institute (2026). *Notes from the Roundtable: Digital Identity as a Crucial Building Block for a Digital Sovereign Europe*. EY Offices, Zurich, Switzerland, 7 April 2026. Invite-only event, 20 participants, under Chatham House Rule. Funded by ENS DAO.

Acharya, A. (2026). Presentation on Bhutan National Digital Identity (NDI): architecture, adoption, and governance. *Roundtable: Digital Identity as a Crucial Building Block for a Digital Sovereign Europe*, EY Offices, Zurich, Switzerland, 7 April 2026. Under Chatham House Rule.

Bouma, T. (2026). Written questionnaire response on the Pan-Canadian Trust Framework (PCTF): design foundations, governance architecture, and interoperability. Interview conducted for the EDI Digital Identity Research Programme, March 2026. Tim Bouma is an Independent Advisor on Digital Identity and former Senior Analyst, Treasury Board of Canada Secretariat; contributor to the Digital Governance Council of Canada and lead architect of the PCTF standards subsequently adopted by ISO.

Bouma, T. (2026). Presentation on the Pan-Canadian Trust Framework (PCTF): federated governance, mutual recognition, and global standard-setting. *Roundtable: Digital Identity as a Crucial Building Block for a Digital Sovereign Europe*, EY Offices, Zurich, Switzerland, 7 April 2026. Under Chatham House Rule.

Goh, C. (2026). Presentation on Australia and New Zealand digital identity update: Digital Trust Reference Architecture, VC-based credential ecosystem, and inclusion challenges. *Roundtable: Digital Identity as a Crucial Building Block for a Digital Sovereign Europe*, EY Offices, Zurich, Switzerland, 7 April 2026. Under Chatham House Rule.

Rauschenbach, R. (2026). Written questionnaire response on Swiyu and the Swiss e-ID: design foundations, functional architecture, minimisation-by-design, and interoperability barriers. Interview conducted for the EDI Digital Identity Research Programme, 27 March 2026. Rolf Rauschenbach is Deputy Head of the eID Unit, Federal Office of Justice, Swiss Federal Department of Justice and Police.

Rauschenbach, R. (2026). Presentation on Swiyu / Swiss e-ID: sovereignty versus autarchy, digital trust infrastructure, and the Global Digital Collaboration initiative. *Roundtable: Digital Identity as a Crucial Building Block for a Digital Sovereign Europe*, EY Offices, Zurich, Switzerland, 7 April 2026. Under Chatham House Rule.

Sharma, P. (2026). Written questionnaire response on the Bhutan National Digital Identity (NDI): design principles, self-sovereign identity architecture, governance, and adoption. Interview conducted for the EDI Digital Identity Research Programme, March 2026. Pallavi Sharma is Chief Operating Officer, Bhutan NDI Limited, a subsidiary of Druk Holding and Investments (DHI).

Varma, P. (2026). Presentation on Aadhaar: design philosophy, privacy-by-design mechanisms, and lessons for global digital identity governance. *Roundtable: Digital Identity as a Crucial Building Block for a Digital Sovereign Europe*, EY Offices, Zurich, Switzerland, 7 April 2026. Under Chatham House Rule. Pramod Varma is Chief Architect, Aadhaar (Unique Identification Authority of India).

II. LEGISLATIVE AND REGULATORY INSTRUMENTS

Australia. *Digital ID Act 2024*, No. 25 of 2024. Commonwealth of Australia. Available at: https://www.legislation.gov.au/C2024A00025/latest/text

Brazil. *Lei n.° 14.129, de 29 de março de 2021 (Lei do Governo Digital)* [Federal Law 14.129/2021, Digital Government Law]. Presidência da República, Brasília. Available at: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm

Bhutan. *National Digital Identity Act of Bhutan, 2023*. Department of Information Technology and Telecom, Royal Government of Bhutan. Available at: https://tech.gov.bt/wp-content/uploads/2024/09/National-Digital-Identity-Act-of-Bhutan-2023.pdf

British Columbia. *Freedom of Information and Protection of Privacy Act (FOIPPA)*, RSBC 1996, c. 165. Province of British Columbia.

British Columbia. *Information Management* Act, SBC 2015, c. 27. Province of British Columbia.

Ethiopia. *Digital Identification Proclamation No. 1284/2023*. Federal Negarit Gazette of the Federal Democratic Republic of Ethiopia.

European Union. *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework (eIDAS 2.0). Official Journal of the European Union*, L, 2024/1183, 30 April 2024.

India. *The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016*. Ministry of Law and Justice, Government of India. Available at: https://uidai.gov.in/en/legal-framework/aadhaar-act.html

Ontario. *Enhancing Digital Security and Trust Act, 2024 (EDSTA)*, SO 2024, c. 24. Legislative Assembly of Ontario. Available at: https://www.ontario.ca/laws/statute/24e24

Republic of Korea. *Electronic Government Act* (as amended, July 2025). Ministry of Government Legislation. Available at: https://www.law.go.kr/LSW/eng/engLsSc.do?menuId=2&query=ELECTRONIC+GOVERNMENT+ACT

Switzerland. *Bundesgesetz über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz) vom 20. Dezember 2024* [Federal Act on Electronic Identity Credentials and Other Electronic Proofs of Identity, E-ID Act]. Federal Chancellery. Available at: https://www.fedlex.admin.ch/eli/fga/2025/20/de

United States. REAL ID Act of 2005, Pub. L. 109-13, 119 Stat. 302 (2005). Available at: https://www.congress.gov/109/plaws/publ13/PLAW-109publ13.pdf

United Kingdom. *UK Digital Identity and Attributes Trust Framework, Gamma 0.4 (Pre-release)*. Office for Digital Identities and Attributes, Department for Science, Innovation and Technology, December 2025. Available at: https://www.gov.uk/government/publications/uk-digital-identity-and-attributes-trust-framework-04/

III. INSTITUTIONAL AND GOVERNMENT DOCUMENTS

Australian Competition and Consumer Commission (ACCC) (2024). *Digital ID Regulation*. Available at: https://www.accc.gov.au/by-industry/digital-platforms-and-services/digital-id-regulation

Australian Digital Transformation Agency (2024). *Australian Government Digital ID System (AGDIS)*. Available at: https://architecture.digital.gov.au/design/agdis

Australian Government, Office of Impact Analysis (2024). I*mpact Analysis: Legislating the Australian Government Digital ID Program*. Department of the Prime Minister and Cabinet. Available at: https://oia.pmc.gov.au/sites/default/files/posts/2024/01/Impact%20Analysis%20%28IA%29%20Regulating%20Expansion%20of%20the%20Australian%20Government%20Digital%20ID%20Program.pdf

Office of the Australian Information Commissioner (OAIC) (2024). *Digital ID*. Available at: https://www.oaic.gov.au/digital-id

Bhutan NDI Limited and Trust Over IP Foundation (2024). *Case Study: Bhutan NDI — National Digital Identity, ToIP Digital Trust Ecosystems*, Version 1.0. Trust Over IP Foundation. Available at: https://trustoverip.org/wp-content/uploads/Case-Study-Bhutan-NDI-National-Digital-Identity-ToIP-Digital-Trust-Ecosystems-V1.0-2024-05-21.ext_.pdf

British Columbia Digital Government (2024). *BC Wallet: Digital Trust Programme*. Province of British Columbia. Available at: https://digital.gov.bc.ca/digital-trust/

British Columbia Digital Government (2024). *BC Wallet Privacy Policy* (updated April 2024). Province of British Columbia. Available at: https://www2.gov.bc.ca/gov/content/governments/government-id/bc-wallet/privacy

Digital Governance Council of Canada (2023–2024). N*ational Standards for Digital Identity and Trust Services (CAN/DGSI 103-0 through 103-4)*. Including: Code of Practice (103-0); Fundamentals (103-1); Delivery of Healthcare Services (103-2); Digital Credential Management (103-3); Digital Wallets (103-4). Available at: https://dgc-cgn.org/standards/

European Commission, Directorate-General for Communications Networks, Content and Technology (2023). *EU-Japan Memorandum of Cooperation on Digital Identities and Trust Services to Implement Data Free Flow with Trust*. Available at: https://digital-strategy.ec.europa.eu/en/library/eu-japan-memorandum-cooperation-digital-identities-and-trust-services-implement-data-free-flow

Japan Digital Agency (2024). *Trust (Digital Identity) Policy*. Available at: https://www.digital.go.jp/en/policies/trust

Japan Digital Agency (2024). *Data Free Flow with Trust (DFFT) Policy*. Available at: https://www.digital.go.jp/en/policies/dfft

Japan Trusted Web Promotion Council (2023). *Trusted Web White Paper*, Version 3.0. Available at: https://github.com/TrustedWebPromotionCouncil/Documents/tree/master/22_white_paper_ver3.0_English

Office of the Auditor General of Ontario (2024). *Annual Report 2024: Digitalisation of Government Services by ServiceOntario* (pp. 30 ff.). Queen's Printer for Ontario. Available at: https://www.auditor.on.ca/en/content/annualreports/arreports/en24/pa_ONdigital_en24.pdf

Ontario Ministry of Public and Business Service Delivery (2021). *Consultation: Policy Framework for Ontario's Digital Identity Programme*. Government of Ontario. Available at: https://www.ontario.ca/page/consultation-policy-framework-ontarios-digital-identity-program

Republic of Korea, Ministry of the Interior and Safety (2025). *National Mobile Resident Registration Card: Full Rollout for 52 Million Citizens* (March 2025). MOIS Digital Government Bureau. Available at: https://www.mois.go.kr/eng/sub/a03/EGovernment/screen.do

Swiss Federal Chancellery (2025). *Swiyu Trust Infrastructure: Technical Documentation and Open-Source Repositories*. Available at: https://github.com/swiyu-admin-ch

Swiss Federal Office of Justice (2025). *Swiss e-ID: Technology and Public Beta Documentation*. Available at: https://www.eid.admin.ch/en/technology

Swiss Federal Chancellery (2025). *Popular Vote of 28 September 2025: E-ID Act*. Federal Council. Available at: https://www.admin.ch/gov/en/start/documentation/votes/20250928/e-id-act.html

Unique Identification Authority of India (UIDAI) (2024). *Aadhaar: Official Documentation and Legal Framework*. Available at: https://uidai.gov.in/

United Kingdom, Office for Digital Identities and Attributes (OfDIA) (2026). *New Digital ID Scheme to Be Rolled Out Across the UK*. Department for Science, Innovation and Technology. Available at: https://www.gov.uk/government/news/new-digital-id-scheme-to-be-rolled-out-across-uk

United Kingdom, Office for Digital Identities and Attributes (OfDIA) (2026). *International Use of Digital Identities and Credentials: Stakeholder Survey Responses*. Department for Science, Innovation and Technology, February 2026. Available at: https://www.gov.uk/government/publications/international-use-of-digital-identities-and-credentials-stakeholder-survey-responses/

IV. INTERNATIONAL ORGANISATION REPORTS AND RECOMMENDATIONS

Global Digital Collaboration Conference (GDC25) (2025). *Book of Proceedings: Global Digital Collaboration Conference 2025. Geneva, July 2025*. Co-organised by the Swiss Confederation and 50 partner institutions. 81 pp.

OECD (2024). *G7 Mapping Exercise of Digital Identity Approaches*. Prepared for the 2024 Italian G7 Presidency. Presented at the G7 Digital and Technology Ministerial Meeting, Como, Italy, 15 October 2024. 30 pp.

OECD (2023). *Recommendation of the Council on the Governance of Digital Identity*, OECD/LEGAL/0491. Adopted by the OECD Council at Ministerial Level, 8 June 2023; updated 2025. Paris: OECD Publishing.

OECD (2025). *Digital Government Review of Korea: Delivering Human-Centred and Proactive Public Services*. Paris: OECD Publishing. Available at: https://www.oecd.org/en/publications/digital-government-review-of-korea_9defc197-en/

OECD (2021). *G20 Collection of Digital Identity Practices*. Prepared for the 2021 Italian G20 Presidency. Paris: OECD Directorate for Public Governance. 86 pp.

OpenWallet Foundation and International Telecommunication Union (ITU) (2025). *Call for Action on Global Digital Trust*. High Level Panel Meeting, World Economic Forum, Davos, 22 January 2025. Hosted by the Swiss Government. 2 pp.

V. ACADEMIC LITERATURE

Bhatt, R., Bhardwaj, R., and Bhardwaj, V. (2020). 'Digital ID capitalism: how emerging economies are re-inventing digital capitalism.' Policy Studies, 42(5–6), pp. 561–580. Available at: https://www.tandfonline.com/doi/full/10.1080/13569775.2020.1751377

Nilekani, N., and Shah, V. (2015). 'India Stack: Digital Infrastructure as Public Good.' *Communications of the ACM*. Available at: https://dl.acm.org/doi/epdf/10.1145/3355625

Supreme Court of India (2018). *Justice K.S. Puttaswamy (Retd.) and Anr. v. Union of India and Ors.*, Writ Petition (Civil) No. 494 of 2012. Judgment of 26 September 2018. Nine-judge bench. Recognised the right to privacy as a fundamental right under the Constitution of India and partially limited mandatory Aadhaar linkage. [Judicial Decision]

VI. TECHNICAL DOCUMENTATION AND STANDARDS

Bhutan NDI Limited (2024). *Open-Source Repositories: Platform, Agent-Controller, Studio, Mediator, Ethereum Schema Manager*. Available at: https://github.com/bhutan-ndi

British Columbia Digital Government (2024). *BC Wallet Mobile: Open-Source Repository*. Available at: https://github.com/bcgov/bc-wallet-mobile

National Institute of Standards and Technology (NIST) (2024). P*ost-Quantum Cryptography Standards: FIPS 203 (ML-KEM), FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA). U.S.* Department of Commerce.

World Wide Web Consortium (W3C) (2024). *Verifiable Credentials Data Model 2.0*. W3C Recommendation. Available at: https://www.w3.org/TR/vc-data-model-2.0/

World Wide Web Consortium (W3C) (2022). *Decentralized Identifiers (DIDs) 1.0: Core Architecture, Data Model, and Representations. W3C Recommendation*. Available at: https://www.w3.org/TR/did-core/

VII. PRESS AND CURRENT AFFAIRS SOURCES

Press sources are cited solely for specific factual claims regarding current events, legislative developments, or system launches where no official primary source was available at time of writing. All URLs verified May 2026.

Baer & Karrer (2025). 'Switzerland says yes to e-ID: Digital Identity is on its way.' Legal update, October 2025. Available at: https://www.baerkarrer.ch/en/publications/switzerland-says-yes-to-e-id-digital-identity-is-on-its-way

Biometric Update (2024). 'New Zealand finalises Digital Identity Services Trust Framework.' November 2024. Available at: https://www.biometricupdate.com/202411/new-zealand-finalizes-digital-identity-services-trust-framework

Biometric Update (2025). 'South Korea's non-compliant digital ID called into question.' August 2025. Available at: https://www.biometricupdate.com/202508/south-koreas-non-compliant-digital-id-called-into-question

Biometric Update (2026). 'Utah passes amendments to State-Endorsed Digital Identity law.' February 2026. Available at: https://www.biometricupdate.com/202602/utah-passes-amendments-to-state-endorsed-digital-identity-law

Daily Bhutan (2025). 'Bhutan makes history as the world's first nation to launch a national digital ID on Ethereum.' October 2025. Available at: https://www.dailybhutan.com/article/bhutan-makes-history-as-the-world-s-first-nation-to-launch-a-national-digital-id-on-ethereum

IDTech Wire (2025). 'Bhutan advances national digital identity: migration to Ethereum blockchain.' 2025. Available at: https://idtechwire.com/bhutan-advances-national-digital-identity-migration-to-ethereum-blockchain/

IDTech Wire (2025). 'South Korea completes national digital ID rollout for 52 million citizens.' March 2025. Available at: https://idtechwire.com/south-korea-completes-national-digital-id-rollout-for-52-million-citizens/

Toppan Holdings (2025). 'TOPPAN, Edge, and Partisia partner on decentralised digital ID with MPC blockchain.' May 2025. Available at: https://www.holdings.toppan.com/en/news/2025/05/newsrelease250507_1.html

Tech Policy Press (2024). 'South Korea's approach to age assurance.' 2024. Available at: https://www.techpolicy.press/south-koreas-approach-to-age-assurance/

World Economic Forum (2023). 'How Japan's Trusted Web can improve digital governance.' January 2023. Available at: https://www.weforum.org/stories/2023/01/how-japan-trusted-web-improve-digital-governance-davos2023/

May 2026

EUROPEAN
DECENTRALISATION INSTITUTE

info@eudecentralisation.org
eudecentralisation.org

Digital Identity as the Foundation of European Sovereignty