

Switzerland's Trek Toward a National Digital Identity System

The nation's experience with developing digital credentials may be instructive for other countries seeking to build an identity system that reflects civic and social preferences.

On September 28, 2025, Swiss voters once again considered a referendum on a national digital identity (e-ID) law passed by Parliament. The government's first attempt at legislating a national digital ID passed in 2019 but was roundly rejected by referendum in 2021, when 64% of voters opposed the law, citing concerns that it delegated operations to private companies. The popular backlash catalyzed years of national deliberation on the question of what kind of e-ID model could meet citizens' demands for transparency, privacy, and security. Parliament passed a redesigned e-ID law in 2024, and this one stood the test of another referendum, but by the thinnest of margins. The new law was supported by just 50.4% of voters.

This referendum back-and-forth is not unfamiliar to the Swiss. By some accounts, Switzerland holds one-fifth of the world's national referendums. Switzerland's direct democracy enables any party that gathers more than 50,000 signatures to launch a nationwide referendum. Combining national, cantonal, and municipal-level referendum initiatives, Swiss citizens vote on around a dozen referendums a year.

What was unique about the e-ID debate was the way it provoked an unusual level of anxiety and mistrust. In a country where people have long relied on the digital world for banking, payments, communications, and travel planning, development of a national digital ID system

brought into sharper focus a broader unease around the digitalization of society. For the Swiss, an e-ID represents more than an app; it is a bellwether for the future of long-cherished rights and values around identity and citizenship in the digital age.

A digital identity is a credential: a set of verifiable attributes backed by an issuing authority that answers the question "With whom am I interacting?" A national e-ID is intended to be the highest-assurance anchor in the digital trust stack, as it would be government-recognized, verifiable across services, and usable for both public and private transactions. As one element of digital public infrastructure, e-IDs—along with digital payment and data-sharing systems—enable trusted interactions across sectors and borders. For example, they can facilitate the efficient delivery of financial, health, and other public services, while supporting private sector competition and innovation.

Originally intended to ensure public trust in an increasingly digital world, the proposition of the Swiss e-ID system ignited a national debate about how that trust is built and how such a system should be used. The question was not only who should hold the keys, but who should get to design the lock. Drawing on our work connecting digital trust research and policy, we believe

Switzerland's e-ID experience exposes underexamined political, social, and technical dimensions of cultivating digital trust through democratic process and deliberation. Its example may be instructive to other countries seeking to refine digital infrastructure services that provide trusted, interoperable, persistent, and legally binding digital identities for citizens.

A circuitous path

The main argument for the passage of Switzerland's 2019 e-ID law was its potential to boost economic growth and connect Switzerland to a digital future. Because other European countries had already established e-ID infrastructure under the framework outlined by the Electronic Identification, Authentication, and Trust Services (eIDAS) regulation of the European Union (EU), the move was seen as an attempt to catch up. The Swiss law built upon past national efforts to secure personal digital information by sector, including a mobile ID from the telecom provider Swisscom, a Swiss Federal Railways' commuter pass, and SwissID, a digital credential for accessing a host of online services available through the national postal service, Swiss

fore, it relied on Apple and Google systems, which many users worried could increase their exposure to unwarranted data collection. A survey before the launch of the app showed high confidence in contact tracing apps issued by the Swiss Federal Council (54%) or the Federal Office of Public Health (33%), with far lower levels of trust in those issued by technology companies (6%). Even though the app allowed individuals to choose whether they wanted to opt in, for some Swiss citizens it exemplified the way they were left out of the design of digital society.

In the months after the e-ID law's passage, a coalition of civil society groups collected 64,000 signatures to launch a referendum that struck down the e-ID law in March 2021. Acknowledging the concerns of its citizens, the Swiss government then embarked on a new pathway to the e-ID, emphasizing transparency, openness, and accountability this time around.

The Federal Council held public consultations to inform a revised e-ID framework, inviting citizens, local governments (cantons), industry, and civil society groups to weigh in on the qualities of a suitable e-ID. This public input would determine the level of privacy the e-ID would guarantee, the

Originally intended to ensure public trust in an increasingly digital world, the proposition of the Swiss e-ID system ignited a national debate about how that trust is built and how such a system should be used.

Post. Each of these prior projects was supported through a public-private partnership. The 2019 law embraced a similar design: The state would approve private companies as identity providers to issue and operate the national e-ID system.

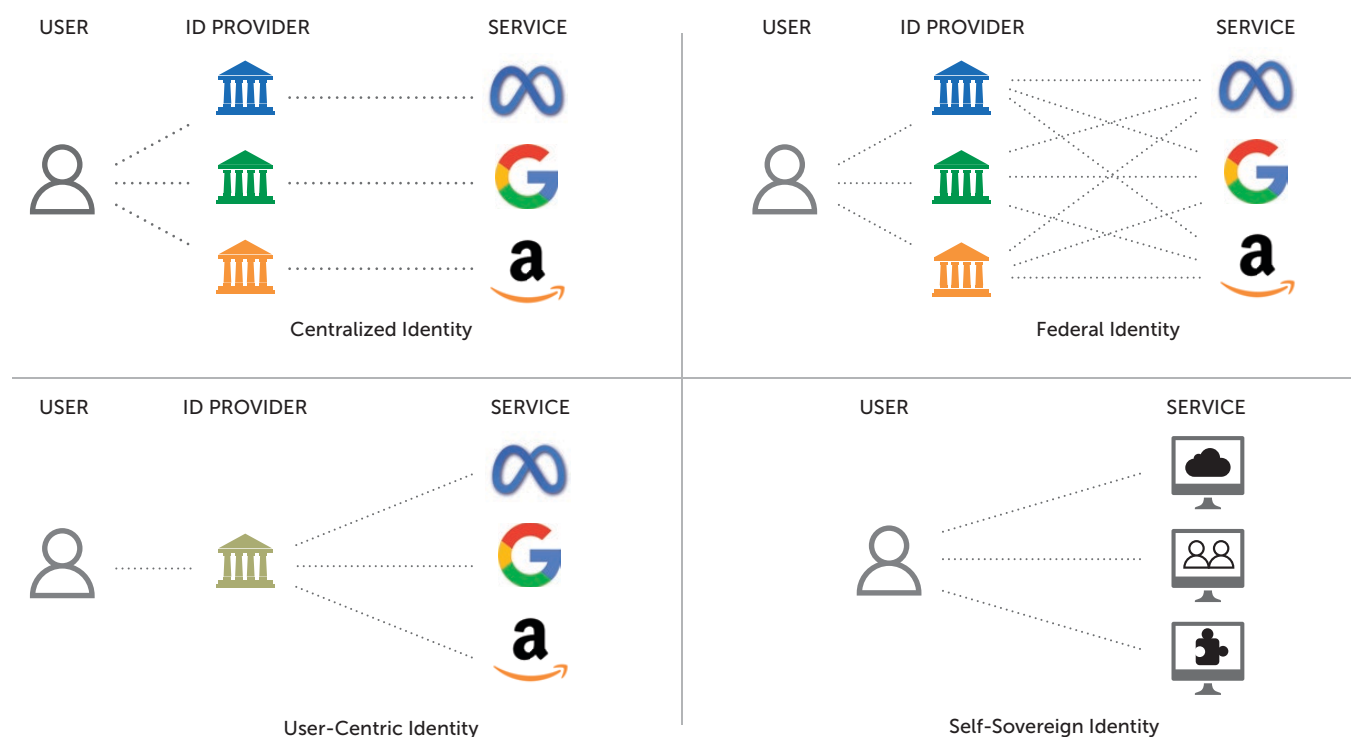
Voter opposition coalesced soon after the law's passage. Opponents argued its purpose was not clear; it failed to ensure citizens' data protection and privacy; and it extended too much control to the private sector, positioning the state as little more than a data provider. Digital rights advocate Olga Baranova of the nongovernmental agency CH++ emphasized to us recently that the lobbying effort was dominated by a coalition of private, state-owned, and partially state-owned companies. Voters were not seriously consulted on the sensitive issue of national identity. The initiative seemed to have gone through the legislative process as if it were an issue belonging to politicians and to industry—not as a matter of public interest.

The COVID-19 pandemic exacerbated these concerns. Although the SwissCovid contact tracing app was developed with privacy-by-design and transparency principles at the

ambition of the broader Swiss digital public infrastructure in which the e-ID would function, and the e-ID's interoperability with the EU's Digital Identity framework. In parallel with consultations, the Federal Office of Information Technology, Systems, and Telecommunication launched an experimental sandbox to allow public and private actors to prototype e-ID implementations, test interoperability and security assumptions, and identify practical trade-offs under supervised conditions. The Center for Digital Trust at EPFL—where we both work—used the sandbox to implement a proof of concept for digital diplomas and then started two projects on the improvement of privacy properties of future implementations of digital identities.

Throughout the consultations and public deliberation that followed, one issue that resonated strongly with Swiss voters was digital sovereignty: Who is actually in control of a country's identity infrastructure? In practice, when no public e-ID exists, social log-ins and single sign-ons from Google, Apple, Microsoft, and Meta perform many identity functions. Without a public alternative, foreign private platforms become de facto identity providers, with control

Figure 1. EXAMPLES OF DIGITAL IDENTITY SCHEMES



over authentication flows, attribute-sharing, and cross-service correlation. For some Swiss voters, that prospect represented an erosion of national control over a core public good.

Designing trust mechanisms for the digital realm

As consultations and sandbox sessions uncovered voters' anxieties about governance, transparency, and oversight, it became clear that voters' opposition to a national e-ID system wasn't a rejection of digital identification altogether—it was a repudiation of the system design. The Swiss government responded by integrating technical safeguards and legal protections into the design of a new law. The participatory process also allowed exchanges between citizens, data privacy experts, and government officials on the benefits of well-designed digital IDs: reliable age verification, improved identity fraud detection, data-sharing limitations on service providers, standardized credentials, and auditability.

Design choices about architecture and privacy of an e-ID determine both functionality and acceptability. Developing an e-ID requires managing trade-offs across a spectrum of factors, including how identity data are stored, who controls the issuing process, and how much direct control users have.

At one end are centralized schemes in which a government (or another operator) holds identity records and controls authentication. Those designs simplify administration and interoperability, but they also concentrate risk and raise

concerns about surveillance and data breaches. At the other end are user-centric or self-sovereign identity (SSI) models, in which individuals store credentials in personal wallets and share cryptographic proofs directly with service providers. SSI ensures privacy from intermediaries but creates practical challenges for recovery, usability, and jurisdictional acceptance. Federated models sit between these poles: Multiple certified issuers operate under common standards, enabling the acceptance of credentials from many providers.

Each of these architectures can have complementary privacy protections layered onto them, limiting how much information is revealed in transactions. These include techniques such as minimal information request, which limits the information the verifier can ask for to perform the service and conform to the law, and selective disclosure, which lets a user reveal only what is necessary (e.g., photo and birth date, but not name and place of birth). Another is unlinkability, which aims to prevent correlating separate transactions to the same person. Zero-knowledge proofs allow a user to confirm that a data point is true without revealing the underlying data (e.g., "over 18").

All four techniques follow the principles of data minimization (the data controller should only collect directly relevant and necessary information and should retain it for no longer than necessary) and proportionality (there should be a balance between the means used and the intended aim),

Figure 2. KEY DESIGN ELEMENTS OF FOUR GLOBAL AND NATIONAL E-IDS

Key Design Element		eIDAS 2.0 (EU)	Aadhaar (India)	Modular Open-Source Identity Platform (MOSIP)	Swiss e-ID
Identity/Wallet		Y	Y	Y	Y
Signatures	Advanced/qualified electronic signature	Y	Y	N	N
	Qualified website authentication certificate	Y	N	N	N
Trust service	Trust service	Y	N	N	N
	European Union Trusted Lists	Y	N	N	N
Payment		N	Y	N	N

Note: MOSIP is an open-source platform designed to help governments build and implement secure, scalable, and interoperable foundational digital identity systems. Inspired by the successful deployment of India's Aadhaar system, developers at the International Institute of Information Technology Bangalore conceived MOSIP as a cost-effective and replicable identity infrastructure solution for developing nations.

both of which are upheld by EU data protection laws. Each technique reduces specific risks, but none eliminates the need for governance. Legal limits, independent oversight, enforcement, and transparent procurement practices remain essential.

Every e-ID architecture requires trade-offs among scale, convenience, privacy, and political acceptability. The model adopted by the Swiss Parliament in December 2024 was designed around a middle path, aiming for compatibility with the EU's Digital Identity Wallet initiative, while explicitly funding research in emerging digital privacy techniques. For the Swiss, interoperability matters for commerce, travel, and cross-border services, but the design does not sacrifice domestic expectations of privacy. At the same time, the design explicitly avoided competing with private sector companies offering digital signatures.

Citizenship in the digital age

After the passage of the second e-ID law in 2024, this one based on SSI, ongoing public debate precipitated another referendum. The most significant, first-order public worry centered on pervasive surveillance and loss of privacy. Many citizens feared that a widely deployed e-ID could make it simple to link actions across government and commercial systems and to create comprehensive, searchable records of individuals' online and offline

interactions. Although the Swiss have relatively strong trust in their government and law enforcement authorities, for some voters the designation of the Federal Office of Police as the issuing authority triggered anxiety about the future of sensitive personal information contained within the e-ID system.

Critics warned of the possibility of mission creep, raising concerns that the initial conveniences of the digital ID could evolve into broader dependence, leading to routine issuance of additional digital certificates for other (not originally intended) purposes. Suggestions such as replacing Swiss supermarket giant Migros's loyalty card with the e-ID illustrated how the credential might spread into everyday commerce. Citizens feared that if the e-ID became the default verification method for age checks, prescription pickups, hotel check-ins, and online purchases, companies and intermediaries could stitch together formerly separate interactions into detailed profiles, which could be used to accelerate global e-commerce but potentially compromise consumer privacy. This scenario was the focus of much of the Global Digital Collaboration Conference, held in Geneva in July 2025. Another concern was whether such detailed profiles would be used to harm or exert digital control over people, whether through price discrimination, exclusion from services, reputational damage, or chilling effects on free expression.

Suspensions remained about the law's promise that the e-ID would stay voluntary, especially if the system evolved beyond a digital identity tool into a broader platform for digital engagement. In a recent conversation with us, Swiss journalist Grégoire Barbey, who covers cyber news for *Le Temps*, cautioned that the e-ID effort represented a shift to a system in which the state actively drives digitalization, thereby increasing societal dependence on systems it does not fully control, without offering a clearly superior value proposition over existing paper-based solutions.

Beyond the politics of the e-ID, a movement for "digital integrity" is taking shape in Switzerland. Its founders call for "a right to be forgotten, a right to live offline, a right to information security, a right to be judged by humans and not by machines, a right to protection against the use of data without consent that affects digital life, and a right not to be measured and monitored." Public debates about digital integrity are taking place across the country, and the right to digital integrity has been added to the cantonal constitutions of Geneva and Neuchâtel.

Despite years of deliberation on the subject, many voters still have questions about the e-ID's value. If a trustworthy

The e-ID also has the potential to make it easier for the Swiss to hold even more referendums. Today, potential secondary applications for the e-ID, including online signature collection and electronic voting, are on the table for discussion.

Having employed its direct democracy through two cycles of law and referendum, Switzerland has gathered rich experience in learning how to build a digital identity system that reflects national civic and social preferences.

The first lesson is that a sustained, accessible public awareness campaign is essential. Concepts and frameworks such as digital credentials, digital public infrastructure, and self-sovereign identity are far outside the average voter's comfort zone. Proponents need to do the work of explaining how it will work, how it will not work, and in which aspects it resembles or differs from other existing systems, including those led by the private sector. Shortcomings and trade-offs should be acknowledged so that the public can be well informed and able to distinguish facts from misinformation.

Second, an open, well-documented process builds legitimacy. Even many Swiss who voted against the second referendum accepted the fairness of the process. Publishing timelines, technical specifications, independent audits, and

Developing an e-ID requires managing trade-offs across a spectrum of factors, including how identity data are stored, who controls the issuing process, and how much direct control users have.

digital infrastructure that guarantees the authenticity of a person's identity, protects anonymity and privacy, and liberates the digital economy is to be realized, what might society be sacrificing for such advancements? Will the trade-off be worth it? What is the added value for any one person? *Why do I as a citizen need an e-ID?*

These questions are still being deliberated, even as the e-ID effort shifts toward implementation and enforcement. The government already proposed measures to strengthen acceptance of the e-ID and ensure that companies are strictly prevented from using unauthorized data or acquiring mass government-verified data. Global interoperability and trust mechanisms will continue to form the crux of future cross-border conversations.

The narrow margin of victory for adopting the Swiss e-ID shows persistent public unease with digitalization, at both practical and philosophical levels. Yet the participatory process mounted by the government to arrive at this victory was a first in Swiss governance. It was a live experiment in uncovering shared public values regarding privacy, agency, and the balance between citizens' on- and offline lives in the modern world.

plain-language summaries helps sustain that legitimacy.

Finally, the design of the e-ID must be informed by citizens' preferences and concerns and shaped by their common vision and goals for a digital future. Establishing an open sandbox environment and offering access to resources like repositories and live demonstrations helped facilitate the iterative development and testing of e-ID solutions. Open debate and deliberation between government officials and their constituents, along with the involvement of civil society, ensure that citizens' concerns—not only about the e-ID but, more fundamentally, about rights to privacy, agency, and digital integrity—can be heard and addressed.

Implementing a national digital identity system may seem like a technical project, but it is as much a political and social one, succeeding only when citizens understand it, trust it, and see themselves and their values reflected in the design.

Katherine Loh is the strategic initiatives lead at the Center for Digital Trust at EPFL, the École Polytechnique Fédérale de Lausanne. **Imad Aad** is the head of government and society relations at the Center for Digital Trust at EPFL.