



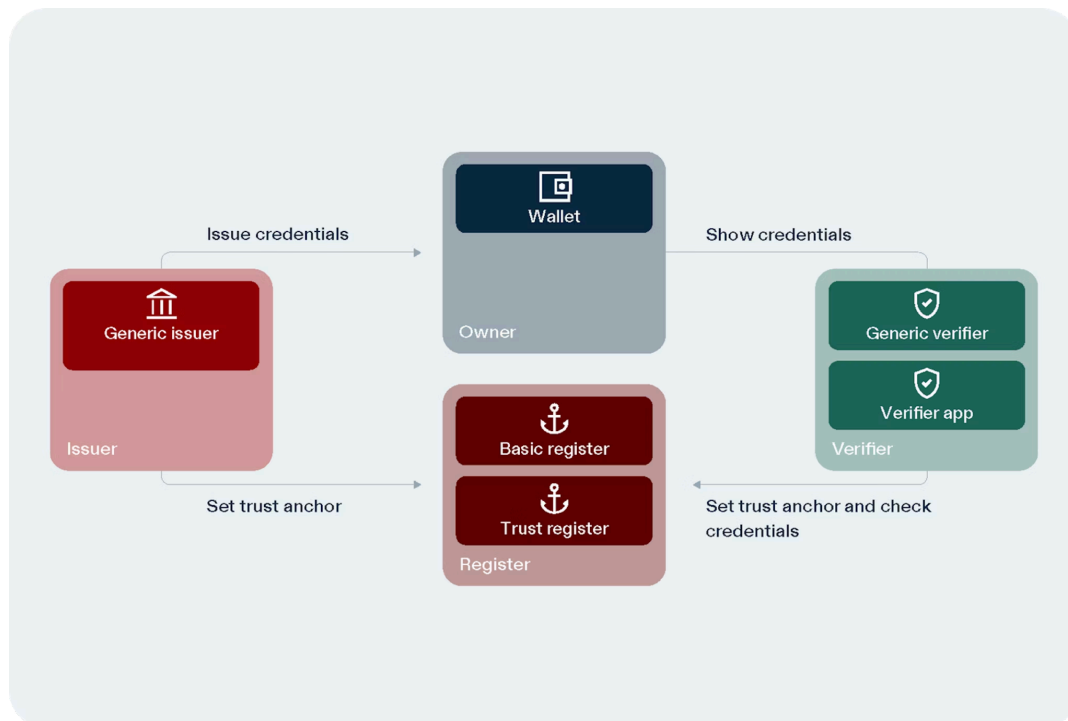
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Digital identity and Trust Infrastructure

Technology

The federal government issues the e-ID and operates the necessary technical infrastructure to enable the secure exchange of digital credentials. This infrastructure is open to anyone who aims to issue, hold or verify such credentials.

(Personal) data from individuals' digital credentials is never stored in these registers. This makes it impossible to link usage data from different credentials and create personal user profiles.



What are the benefits of the state-issued e-ID and the Trust Infrastructure?

The state-issued e-ID addresses the lack of secure, privacy-preserving, userfriendly and legally recognised digital proofs of identity for online interactions with businesses and public authorities.

The e-ID and its Trust Infrastructure establish a digital foundation of trust that gives residents of Switzerland and Swiss citizens abroad full control over their personal data. It enables seamless and secure interactions in a connected digital society, paving the way for innovative, privacy-friendly services and a modern, efficient Switzerland.

Developing and Learning Together

The architecture model explained briefly

The e-ID architecture is based on a **decentralised identity model** that gives users full control over their identity and personal data. There is **no central authority** that aggregates, stores or controls credentials. Data flows occur **directly** and in a **decentralised** manner between the holder and an issuer or verifier. Linkability of usage across different services is technically restricted. Interactions between different actors also cannot be directly linked. During a verification process, the holder shares only the necessary data directly with a verifier, without the issuer being informed.

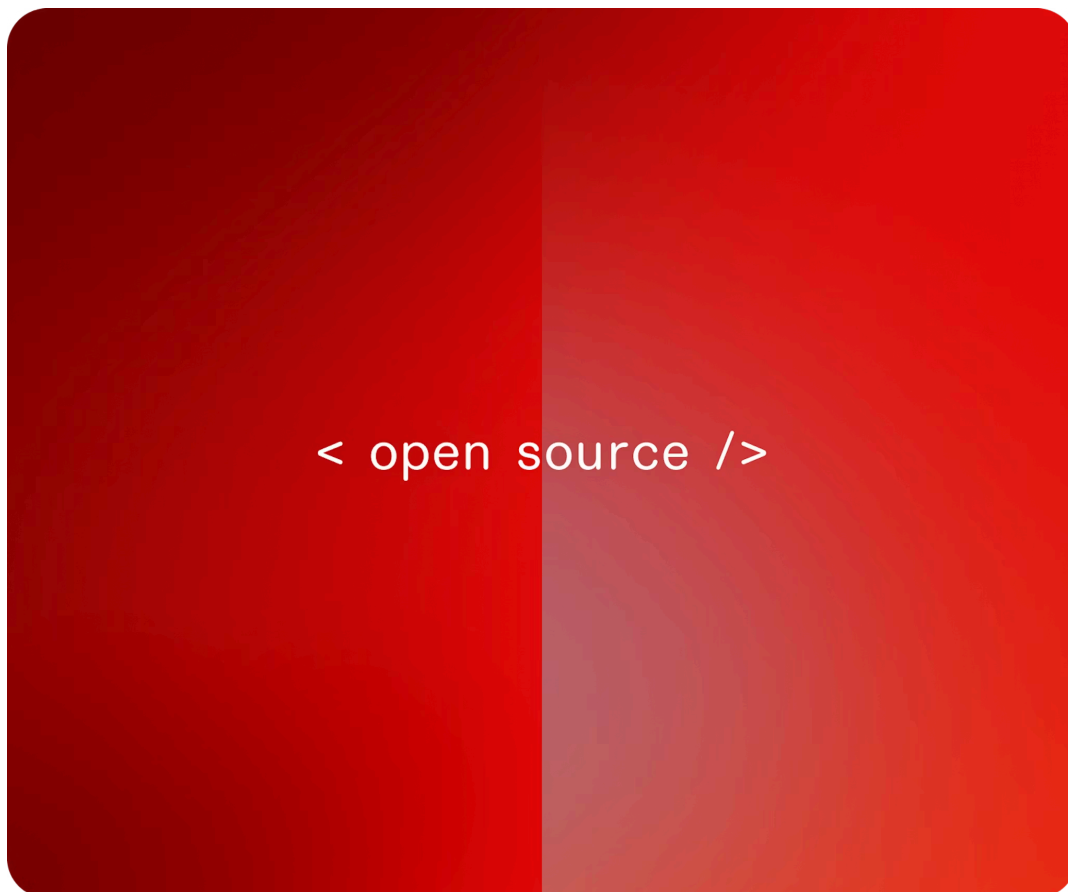
To verify the authenticity and validity of digital credentials, the federal government operates a Base Registry and a Trust Registry. These registers primarily store the identifiers and public keys of credential issuers and verifiers, information on their trust level, as well as information on a credentials state of revocation. Personal data contained in individual digital credentials is never stored in these registers.

The system uses **open standards** such as Verifiable Credentials (SD-JWT VC), Decentralised Identifiers (DIDs), as well as OpenID for Verifiable Credential Issuance (OpenID4VCI) and Verifiable Presentations (OpenID4VP). Mechanisms like selective disclosure and batch issuance ensure privacy and allow to reduce shared identity data. The architecture is designed with interoperability, security, and privacy in mind.

[Technical documentation](#)



Transparency through open source



The e-ID infrastructure is based on open standards and developed according to the open-source principle. The source code is publicly available on GitHub for anyone to inspect. This ensures full transparency on how the system works at any time. To identify potential vulnerabilities and improvements in the code, bug bounty programs are carried out.

[Github](#)

Public Beta: Practical Testing

The public beta of the Swiss e-ID is an open testing phase where authorities, businesses and private individuals can explore the digital identity solution for the first time under real-world conditions. During public beta, the swiyu Wallet is available with sample identities, allowing all participants to test the process...

Successful Pilot: The Electronic learner driver permit (eLDP)

As part of the development of the e-ID and the Trust Infrastructure, the federal government is gaining practical experience through concrete pilot projects. The ePDL makes it possible to test the planned e-ID Trust Infrastructure with real users and to learn from their feedback.

Involvement of Academia, Civil Society and Industry



The federal government is developing the e-ID and the Trust Infrastructure in dialogue with interested parties from academia (e.g. ETH Zurich, EPFL), civil society and industry. The shared goal is to create a democratically supported, voluntary, secure and user-friendly solution for everyone. The government provides regular updates on the progress of the project and takes feedback from the public, academia and industry into account. Currently, the e-ID project team sits on the Governmental Consultative Committee of the [Open Wallet Forum](#) working together with other countries to make digital credentials usable internationally.

Participation

Agile Development and Cross-Authority Collaboration

More than 80 people from various disciplines are currently working on the development of the e-ID and the Trust Infrastructure required for its operation. The development follows an agile approach based on SAFe (Scaled Agile Framework).

The e-ID Project Organisation is headed by Michael Schöll, Director of the Federal Office of Justice (FOJ). The principal authorities involved are:

- Federal Office of Justice (FOJ): Responsible for the legislation and commissioning the Trust Infrastructure
- Federal Office of Information Technology, Systems and Telecommunication (FOITT): Develops and operates the Trust Infrastructure and the mobile app
- Federal Office of Police (fedpol): Issues the e-ID
- Federal Roads Office (FEDRO) and Association of road traffic offices (asa): Issues electronic credentials in the road transport sector
- Digital Public Services Switzerland (DPSS) and **Federal Chancellery (FCh)**: Provides the authentication service of the Swiss authorities (AGOV) and coordinates with communes, cities and cantons.

