AUDIT

Audit of the key project e-ID

Federal Department of Justice

Federal Office of Police fedpol

Federal Office of Information Technology, Systems and Telecommunication

KEY FACTS

The SFAO audited the electronic proof of identity (e-ID) programme for the second time. In this audit, the SFAO assessed the "e-ID issuance" and "trust infrastructure" projects, and the technical design of the Swiss e-ID's IT security. The Federal Office of Justice (FOJ), the Federal Office of Police fedpol and the Federal Office of Information Technology, Systems and Telecommunication (FOITT) are responsible for implementing these projects. The trust infrastructure refers to the technical platform provided by the federal government for the processes associated with the use of a Swiss e-ID. The trust infrastructure is designed to be open so that other electronic proofs of identity can also be integrated into it.

Approximately CHF 182 million was approved for developing and operating the trust infrastructure, issuing the e-ID and pilot projects. Once the project is complete, annual operating costs of around CHF 25 million are expected. At the time of the audit, the Federal Act on Electronic Identity and Other Electronic Credentials (e-ID Act) was subject to a federal popular vote on 28 September 2025. The test version of the "Public Beta" e-ID and the "swiyu" mobile phone app have been running since the end of March 2025. Swiyu allows users to store electronic credentials such as e-IDs and present them digitally when making transactions.

The programme still has a number of key tasks to complete before the earliest possible launch of the e-ID in the third quarter of 2026. The SFAO is concerned about the number of issues still outstanding in the programme. It sees a risk that the stabilisation phase planned for the end of the programme could be misused as a time reserve for unplanned development or corrective work. Since, for risk reasons, the error-free nature and maturity of the product are more important than its timely introduction, the SFAO recommends that the stabilisation phase at the end be maintained in full. This should be done even if it means postponing the introduction of the e-ID.

There are no plans to verify the legitimacy of e-ID checks

The Swiss trust infrastructure for the e-ID and other electronic credentials is still under development. Its core elements are the basic register and the trust register: the basic register contains revoked proofs and all registered participants. Issuers and verifiers who want to instil a high level of trust in users can voluntarily have their identity checked in more detail by the FOJ. If the result is positive, a corresponding entry is made in the second register, known as the trust register. The swiyu app, which can be used by all users for electronic credentials, indicates during a transaction when the identity of the other party has been positively entered in the trust register.

In addition, the necessary legal and technical precautions are being taken to enable in-depth verification of the identity of not only the participants but also the legitimacy of a verifier to check the e-ID. However, the programme currently plans to refrain from using positive trust register entries for verified authentication purposes. This is to avoid complicating the use of the e-ID through official checks, to save participants costs and effort, and to avoid the perception that individual participants are more trustworthy than others.

However, the EFK considers it important that the trust register established under the e-ID Act clearly indicates which purposes for checking the e-ID are legitimate. It therefore recommends that the programme provide for and apply a voluntary process for checking the legitimate purposes of verifiers and the corresponding positive trust register entries for the e-ID.

The encryption of user data has not yet been fully designed and integrated

Communication between the various parties involved in the Swiss e-ID ecosystem is encrypted using standard technical methods. However, these are not always sufficiently secure against attacks by unknown parties, in particular due to the untrustworthy structures of modern anonymous data transport networks. It is therefore necessary, and also planned as part of the programme, to end-to-end encrypt the e-ID user data transmitted between participants. The EFK welcomes this measure, but is surprised that the relevant concept for e-ID user data encryption has not yet been finalised and that its development is still pending in the trust infrastructure project. The plans stipulate that this task should be completed by the end of 2025.

The Public Beta test version only partially reflects the future e-ID

The current Public Beta test version includes Beta ID processes developed specifically for demonstration purposes. The future e-ID processes will incorporate the principles of the Beta ID, but are still under development. A key issue that remains unresolved is the completion and integration of fedpol's e-ID issuance processes (unlike a beta ID, which can be created at the touch of a button, the e-ID requires an issuance process).

In its current phase, the trust infrastructure project is focusing on developer and integration tests. Furthermore, all newly developed functions are first checked using penetration tests before being released. A concept for end-to-end testing of the e-ID is already in place, but the specific test cases still need to be created. These user tests are primarily planned for spring 2026 onwards.

Productive operation still needs to be prepared and sufficiently tested

The programme envisages a phase for stabilising and finally approving the overall e-ID system in summer 2026. Productive operation must also be in place by this phase at the latest. It makes sense to identify the operational requirements in advance and to test measures as extensively as possible in the Public Beta version. However, in addition to the development work that still needs to be completed and the end-to-end tests that have yet to be set up, this increases the general time pressure on the programme.

While this is to a certain extent part of any normal project, the SFAO sees a risk here that the time planned for stabilisation in summer 2026 could be reallocated in favour of ongoing development work or troubleshooting. The EFK therefore recommends that the FOJ ensure that sufficient budget, time and personnel are made available in the programme planning for an effective stabilisation phase and for setting up operations. As a consequence, this may mean that the e-ID could be launched later than planned.