

eID Mark II

Christian Grothoff

Berner Fachhochschule

27.2.2025

The E-ID Law (BGEID) - Art 1

Objectives to be assured:

- ▶ Privacy via technology and by default
- ▶ Data security
- ▶ Data minimization
- ▶ Decentralized storage
- ▶ Auditability and reusability
- ▶ Issued and revoked under state authority

The E-ID Law (BGEID) - Art 2 & 3

Personal data created when the base register or trust register are **queried** can be:

- ▶ **recorded**
- ▶ **evaluated** in pseudonymized, and
- ▶ **evaluated** without pseudonymization.

based on RVOG “for security” (RVOG Art 57, d/n/o), invoicing, etc.

The E-ID Law (BGEID) - Art 4

- ▶ The government **may** operate systems that protect the privacy of the identity subjects.

Eh, what? “**may**”?

The E-ID Law (BGEID) - Art 6

- ▶ The issuers **may** revoke any certifications they create.

No rules for that needed?

The E-ID Law (BGEID) - Art 10

- ▶ The base and trust register operator (BIT) *does not* (!) learn the contents of the attestations, **except** from the data generated by the queries.

Does not is an odd formulation. Must not would be better. The queries may leak **everything**.

The E-ID Law (BGEID) - Art 12 & 26

- ▶ The source is shared with public, except if it is **proprietary** or **insecure**.
So it's not actually FLOSS, and likely most not actually shared source either.

The E-ID Law (BGEID) - Art 15

- ▶ Data stored includes **biometrics**
- ▶ Data is not adequate for KYB
- ▶ Data is not compatible with eIDAS (no civil status, educational qualifications, licenses, titles, mandates, etc.)

So it's **more sensitive** data than eIDAS, but not **compatible** and **less useful**.

The E-ID Law (BGEID) - Art 17

- ▶ Onboarding online against AI for free, or
- ▶ onboarding in-person for cash.

Insecure first, pay later.

The E-ID Law (BGEID) - Art 17 & 31

- ▶ Onboarding online against AI for free, or
- ▶ onboarding in-person for cash.

Insecure first, pay later (nudge nudge nudge).

The E-ID Law (BGEID) - Art 19

- ▶ Only a single eID is allowed
- ▶ Exact **secure** revocation process unclear

You must always carry the **same** smartphone (easier to track), and you must participate so you may learn about ID theft.

The E-ID Law (BGEID) - Art 22

- ▶ You need to do everything to prevent and report abuse.

You must thus install some **proprietary** software on a **proprietary** phone and then are **responsible** for all consequences and lack the necessary **understanding** for a proper legal defense.

The E-ID Law (BGEID) - Art 27

- ▶ Your identity data is stored for **20 years**
- ▶ Your biometric data is stored for **5 years** after expiration

Banks “only” store for **10 years**. Data minimization indeed.

E-ID & EPD

- ▶ Mandate for health personal to use E-ID to access EPD
- ▶ Mandate for patients to use E-ID to access their EPD

So much for **voluntary**.

E-ID & qualified electronic signatures

- ▶ E-ID sufficient for QES onboarding by private entities
- ▶ Offered by same commercial entities rejected previously

Best of luck to you, if someone manages to steal your E-ID.

The E-ID Law (BGEID) — Summary

- ▶ Not best possible security for onboarding
- ▶ Not actually FLOSS
- ▶ Not actually decentralized
- ▶ No actual data minimization
- ▶ No real privacy-by-design required
- ▶ No mandate for industry to support citizens without E-ID
- ▶ No mandate to support platforms other than Apple and Google

E-ID Debate

“EID should be like a toothbrush: I have to take it out every day, use it every day, and somehow create value for myself every day.” – Daniel Säuberli (DIDAS)

E-ID Debate

“EID should be like a toothbrush: I have to take it out every day, use it every day, and somehow create value for myself every day.” – Daniel Säuberli (DIDAS)

“I expect that wallets in the future will have a similar complexity to browsers. Browsers are extremely complicated, very time-consuming and very expensive to develop. There will be few wallets because you can hardly make money with them.” – Rolf Rauschenbach (BJ)

E-ID Debate

“EID should be like a toothbrush: I have to take it out every day, use it every day, and somehow create value for myself every day.” – Daniel Säuberli (DIDAS)

“I expect that wallets in the future will have a similar complexity to browsers. Browsers are extremely complicated, very time-consuming and very expensive to develop. There will be few wallets because you can hardly make money with them.” – Rolf Rauschenbach (BJ)

“We don’t preach 100% security. We do a facial image comparison.” – Rolf Rauschenbach (BJ)

E-ID Debate

“We are taking control of this important process.” – Daniel Säuberli (DIDAS)

E-ID Debate

“We are taking control of this important process.” – Daniel Säuberli (DIDAS)

“We are making ourselves dependent on the device manufacturers and operating system manufacturers. This is a compromise for user-friendliness.” – Rolf Rauschenbach (BJ)

SSI Principles

An SSI ecosystem shall ...

- ▶ ... not require **reliance on a centralized system** to represent, control, or verify an entity's digital identity data.
- ▶ ... not restrict the ability of identity rights holders to **move or transfer** a copy of their digital identity data to the agents or **systems of their choice**.
- ▶ ... empower identity rights holders to secure their digital identity data at rest and in motion, to control their own identifiers and encryption keys, and to employ **end-to-end encryption for all interactions**.
- ▶ ... not **require** an identity rights holder **to participate**.
- ▶ ... provide the means for any entity—human, legal, natural, physical or digital—to be represented **by any number** of digital identities.

Recommendations

E-ID should be:

- ▶ voluntary, without financial disadvantages or exclusion for non-participation
- ▶ secure, without compromising for convenience or cost
- ▶ privacy-preserving, with FLOSS, mandatory cryptographic protections and no loopholes