# DIDAS Statement for E-ID Technology
# Discussion Paper

Submitted and published to:
E-ID Team & via www.DIDAS.swiss blogpost

Submitted by:
Digital Identity and Data Sovereignty Association (www.didas.swiss)
Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz
info@didas.swiss

Dear E-ID Team, dear Ladies and Gentlemen

As a continuation of our form-submitted statement on the discussion paper for the «Initial technological basis for the Swiss trust infrastructure», we would like to thank you for the opportunity to comment in an extended format.

The «Digital Identity and Data Sovereignty Association» (DIDAS) is a Swiss non-profit association that was founded with the aim of «Establishing and promoting Switzerland as a leading ecosystem in the development and implementation of privacy-enhancing technologies, services and products that preserve and apply digital identity and electronically verifiable data».

We appreciate the Federal Administration's open approach and the high quality of the draft legislation as well as the technology discussion document. In addition, the understanding and application of a principle-based, iterative, and collaborative approach as critical success factors for the planning and implementation of a sustainable trust infrastructure, the establishment of an electronic identity and other digital proofs, as well as their widespread adoption and use, must be acknowledged.

We are very pleased that DIDAS and its members have been able to make a valuable contribution to the clarification process. This statement is a joint effort by all members of the DIDAS association under the leadership of the executive board. However, to illustrate the weight of DIDAS, we are pleased to explicitly name some of the contributing individuals below (in alphabetical order):

- Michael Doujak, DIDAS, working group technology; Ergon Informatik AG, Product Manager
- Marco Dütsch, DIDAS, working group technology; IKEA, Lead AI Innovation Lab
- Pascal Gottret, DIDAS, working group lead supply chain; Meraxis Group, Head SAP Application Management
- Georg Grewe, Vereign AG, CEO
- Dr. Peter Janes, DIDAS, working group lead health; Abdagon AG, Founder and CEO
- Dr. André Kudra, ESATUS Schweiz AG, CIO
- This Loepfe, DIDAS, working group lead technology a.i.; Verein cardossier, CTO
- Daniel Saeuberli, DIDAS, president; Accelerate GmbH, Founder and Managing Partner
- Vasily Suvorov, DIDAS, board member, working group technology; movos, CTO
- Kai Wagner, DIDAS, working group lead public sector; Procivis AG, Head of Products and Partners
- Prof. Dr. Tim Weingärtner, Lucerne University of Applied Sciences and Arts HSLU

- Richard F. Zbinden, DIDAS, working group technology; Rigiblue®, Founder and CEO

We continue to proudly advocate for SSI principles, as an important north star on this journey.

Rotkreuz, February 2024

Daniel Säuberli
President

Tim Weingärtner
Vice President

Diego Benz
Board Member

Marco Dütsch
Board Member

Ursula Sury
Board Member

Vasily Suvorov
Board Member

# Additional Considerations to the Feedback on the Technology Discussion Paper

The goal of the «Discussion Paper: Initial technological basis for the Swiss trust infrastructure» is to determine the basic technology of the future trust infrastructure the E-ID will be issued to. The paper limits itself to the credential format and the protocols required to exchange such credentials.

While this focus on the very basis of the technology stack allows for a more targeted discussion and decision, it also loses some of the relevant aspects that determine if the technology is fit for purpose.

In our discussions at DIDAS, we have come up with an approach that considers the purpose for which the E-ID and other verifiable credentials are intended to be used. In the following additional considerations, we outline why we believe that such an approach is viable and should be considered as the technology stack of Switzerland's trust infrastructure.

In addition to the technological aspects of our official response, this document aims to convey important considerations to a wider, less technological target audience.

## No pure scenario A or B decision possible

After intensive discussions within and across the working groups, it became clear that both scenarios have technological shortcomings, such that the requirements for the E-ID in accordance with paragraph 2.1 of the technology discussion paper cannot be fully met.

As a result, we have come to realize that a simple decision in favor of one of the proposed scenarios is not enough and therefore cannot be supported.

Whenever a decision cannot lead to a viable solution, the framework conditions may need to be challenged or the proposals must be extended accordingly. This is what we did at DIDAS and tried to enrich the two scenarios technologically to make a clear statement within the framework or to formulate a target-oriented recommendation. In this respect, in addition to answering the questions, we have also drawn up this additional statement. The officially form-submitted response with our «A+» recommendation can be found in the appendix.

# The need to act now

It is important to note that, even with the proposed measures, scenario A+ is still far from ideal. The concerns around over-identification, linkability of credentials usage leading to correlation of identity and potential profiling, are hard to avoid completely with the currently available technologies and respective trade-offs. At the same time, the introduction of reusable electronic identity tools and their usage in corresponding systems is accelerating globally and it is, therefore, better to lead and establish a basis of a sovereign infrastructure, before other solutions take root, that might not be closely aligned with our Swiss values.

Scenario A+ is aligned with the direction that EU is taking and represents a reasonable compromise, which will allow us to gain valuable, first-hand experience with real use-case, understand limitations of the current and properly evaluate emerging technologies.

It is, consequently, an integral part of this proposal that A+ is seen as an intermediate **starting point** that allows for iterative, continuous further development and improvement of the technological infrastructure. We expect that the suggestion described in the section «Opportunity Switzerland» will be viewed as the unalienable part of our proposal moving forward.

# Current state of technology – what is possible, what isn't?

A key requisite for qualified digital identities is cryptographically safe owner binding. Technically, this requires cryptographic primitives «in silicon» in secure elements of devices (typically mobile phones) to prevent any type of misuse or owner faking.

Specifically, the private / public key pair must be generated «in silicon» of the secure element of the device, and the private key must never leave the secure element to prevent any case of misuse by copying the private key. Such technology is a mandatory prerequisite for qualified credentials and thus the E-ID (this was also the case for prior implementations with the same level of trust).

This technology is available for scenario A, but presently not supporting scenario B. Based on current research, hardware support for BBS+ curves, as suggested in scenario B, is not expected to be available within the next five years, due to technology uncertainties as well as the weaker community effort behind it.

# Ways to be ready by 2026

Although (unfortunately) not explicitly stated in the draft of the E-ID act (BGEID), certain relevant use cases, such as registering for the national electronic health record (EPD) or legally binding digital signatures, require qualified digital identities based on current law.

This implies that qualified digital identities and hence credentials are a mandatory requirement for the E-ID, scheduled to be available by 2026. Consequently, this requirement rules out scenario B for qualified credentials until 2026 because cryptographic libraries in software for BBS+ are insufficient for qualified credentials.

While we recommend to closely monitor developments in this area for safe alternatives, this leaves us with scenario A for qualified credentials.

To avoid criticism of opponents in the political process, mitigating measures must be taken to address known weaknesses of the technology as much as possible, hence we converged on scenario A+. Specifically:

- To enforce this approach, only certified wallets shall be permitted to receive a qualified E-ID. Such certified wallets ensure that only authorized verifiers can obtain a qualified E-ID and potentially also limit the set of claims an authorized verifier may request.
- Ephemeral credentials – to allow the private sector to benefit from the new E-ID, we propose to complement the qualified E-ID with a number (e.g. 100) substantial and less restrictive E-IDs.

With these measures in place, the shortcomings of scenario A will be mostly addressed, and both government and private sector use cases can benefit from identities provided by the most trustworthy source for identity information.

Implementing both scenarios, A and B in parallel for the coming two years (as has been discussed internally) would incur substantial complexity for all issuers and verifiers. This would increase the project risk and it would endanger the envisioned availability by 2026.

It is our recommendation to focus on scenario **A+ with its proven technology as initial technology basis for Switzerland's E-ID trust infrastructure**, and we are putting emphasis on key extensions to consider in the financing package of the project.

Further, to cater for technology developments in this fast-moving field, the trust infrastructure **must be designed with its evolution in mind, right from day one.** It is to be designed based on a modular architecture and technology stack as well as multi-protocol support, so the platform can be continuously improved and expanded to other relevant technologies such as mDL, JSON-LD, BBS+, etc. as per the general technological availability and adaptability, as well as key societal, public, and private stakeholders' needs. We recommend establishing a governance body as part of a wider framework, to help guide this evolution.

## Coexistence of Qualified and Substantial Credentials

The **qualified E-ID** is applicable for a limited number of use cases where a high level of trust is required. The qualified E-ID shall be limited to specifically authorized and trusted verifiers, limiting over-identification. The heightened privacy requirements incur explicit user confirmation of every proof request, reducing user experience and convenience to some extent.

Each **substantial E-ID** (of the ephemeral certificates) is intended to be used in only one context to prevent linkability across verifiers, fully transparent to users. Substantial E-IDs shall also have some claims removed (e.g. AVS13) to again reduce the risk of privacy issues.

A less restrictive substantial E-ID is sufficient for most private sector use cases. It allows private keys to be stored without the need of secure elements on devices and cryptographic primitives «in silicon», and therefore offers more convenient solutions for use cases like automating proof requests based on personal preferences and policies, migrating to a new device, or using multiple devices in parallel. In all other aspects (e.g. cryptographic algorithms, credential formats) the substantial E-ID uses the same technology as the qualified E-ID and therefore simplifies the implementation of A+ for verifiers that use both the qualified E-ID and other verifiable credentials.

## Ensuring Trust

The key requirement of a trust infrastructure with the associated ecosystem is to enable verifiability and therefore authenticity of data through human and cryptographic trust. While on a more holistic level, further requirements arise that must be addressed by a governance framework, to ensure this key aspect, some governance and technical measures must be taken within the narrow scope of the discussion paper:

- Every verifier of the ecosystem must be identifiable. Different levels of identification shall be possible, ranging from large commercial participants down to volunteers of hobby associations. Heightened trust levels might require pre-registration or even certification. Different levels of identification will also imply multiple trust registers.
- Proof requests raised against holder wallets shall be logged by the wallet, including requested claims. Proof requests shall be signed to ensure non-repudiation.
- Based on logged proof requests, the holder shall be able to report over-identification attempts (and other patterns or bad practices) of verifiers to an official agency

(anonymously verified or in his name) with minimal effort (by clicking «report» or similar).

## Conclusion «Opportunity Switzerland»

Swiss citizens generally trust their federal government and its practices, a level of trust that may not be present in other countries. Therefore, it is important that we establish a **balanced foundation that yields swift results AND aligns closely with our core values**. The infrastructure shall be designed to utilize the most powerful methods and mechanisms available at any given time, that protect privacy, prevent correlation and linkability, while also being sustainably operable and adaptable by the public and private sectors and civil society.

Digital Identity and trust infrastructure capabilities are **key enablers of the Swiss digital economy**, so it must be recognized that their **adoption within businesses requires special emphasis and systematic support.** A trustworthy and diverse set of services inside the wallet app(s) is vitally important for the adoption by society and the creation of socio-economic value. A systematic approach to these aspects of adoption support must be planned for.

One of Switzerland's superpowers, is its **national ability to contribute to develop, evaluate and adopt new cryptographic primitives through its excellent research facilities**. The approach presents an opportunity for Switzerland to take a leading role in this field, to actively contribute to the decision making of standardization bodies and hardware manufacturers and, potentially, fellow European governments. Independent research helps to level the playing field and reduce dependencies on large technology corporations and foreign research institutions like NIST.

Not being an EU member, Switzerland has less dependencies on other stakeholders and has hence the flexibility to **leap ahead and gather practical experiences** with the emerging trust technologies, from which all stakeholders will benefit in the long run.

## Appendix

Official response submitted by DIDAS.

# DIDAS Responses to Consultation Questions

## Which scenario would you prefer?

Scenario A

## For what reason do you prefer that scenario?

### Clarifications

Scenario A **must** implement mandatory extensions to mitigate known shortcomings (hereinafter referred to as A+):

- Issuing credentials in separate variants:
  - Qualified – mainly for official purposes, stricter, i.e. with identification process, strong cryptographic holder binding in hardware, etc.
  - Substantial – mainly for commercial purposes, less strict owner binding, more convenient.
- Addressing unlinkability by using ephemeral credentials (i.e. dynamically generated credentials, in this context with no or restricted reuse).
- Architecture must be multi stack capable to facilitate evolution (scenario B, mDL and other options).
- Financial coverage must be ensured for **all** mandatory extensions.

### Reasons

- Pragmatic
- Proven technologies
- Large communities
- Lower complexity and project risk
- Doable until 2026
- Achieves important privacy and security requirements if amended in listed areas (i.e. ephemeral credentials, privacy preserving revocation, etc.).
- EU compatible
- Mandatory extensions to avoid potential criticisms in the political process.

# Do both scenarios fulfil your expectations?

No

# What major risks do you foresee?

### Clarifications expectations

- Both scenarios have weaknesses
- A+ is the approach which minimizes weaknesses and complexity and therefore keeps the implementation risk of the project manageable.

### Risks

- Additional complexity of A+
  - Parallel credential issuing
  - Higher UX complexity due to credential variants – must be hidden from users
  - Ephemeral credentials
- Financing does not cover mandatory extensions of A+ scenario.
- Other options (e.g. scenario B, others) will either be never realized or only with a significant, undesirable delay.

# Which «red lines» should not be crossed? Where is no compromise conceivable for you?

- Gaps in privacy preservation for qualified credentials.
- Not providing a qualified level (in what form soever), as this would prevent achieving the political goals for the national E-ID.
- Not providing substantial level, because this would negatively impact adoption by the private sector.
- Inflexible technical specifications and technical infrastructure which prevents evolution as the field progresses.
- Weaking SSI principles which could prevent an ecosystem of credential issuers and verifiers (ambition Level 3).

# Additional remarks

Using qualified and substantial in parallel must be complemented with additional measures:

- A mechanism to ensure that only authorized verifiers are allowed to request qualified credentials, e.g. government bodies, healthcare organizations, financial institutions, etc.
- E-ID must be provided both as qualified and substantial credential. The substantial E-ID shall only contain a subset of claims (e.g. AVS13 not included).

Switzerland shall seize the opportunity to establish focused research and implementations for developing and progressing cryptographic technologies, leading the field and contributing to international decision making.

More in-depth information is provided in our separate statement document.

# Official Sender

DIDAS – Digital Identity and Data Sovereignty Association

Campus Zug Rotkreuz
Surstoffi 1
CH-6343 Rotkreuz

# Your Email

info@didas.swiss