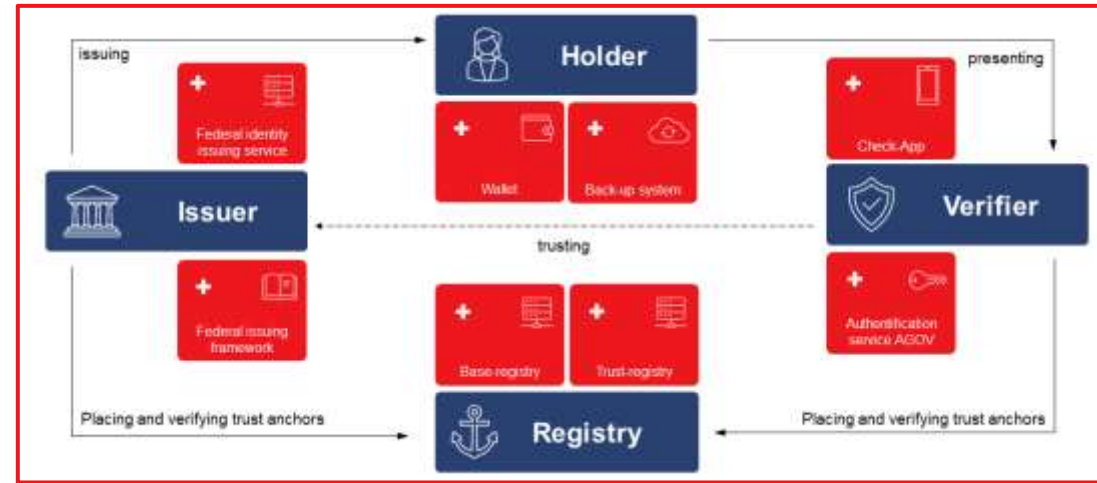E-ID

Discussion Paper: Initial technological basis for the Swiss trust infrastructure

Christian Heimann, FEDPOL | Andreas Frey Sang, BIT
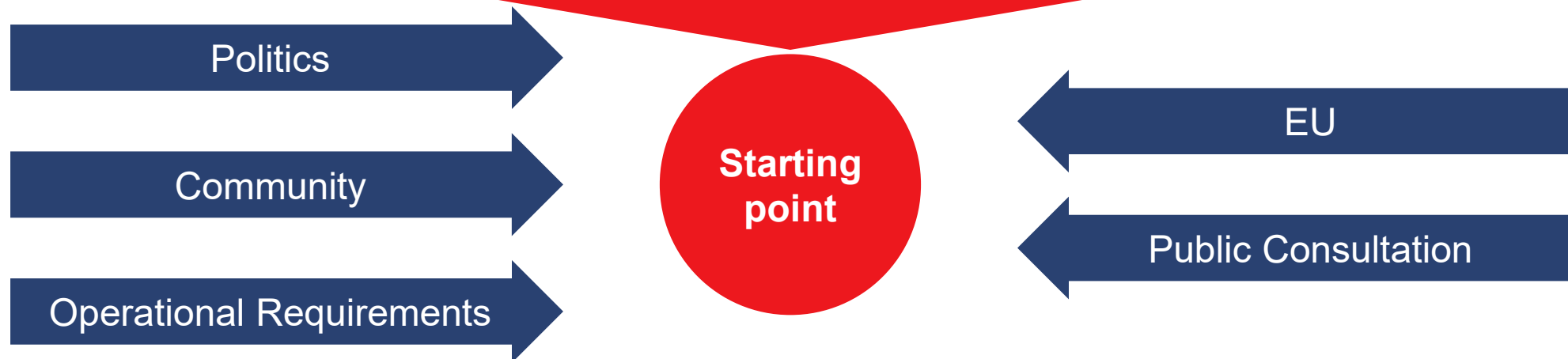
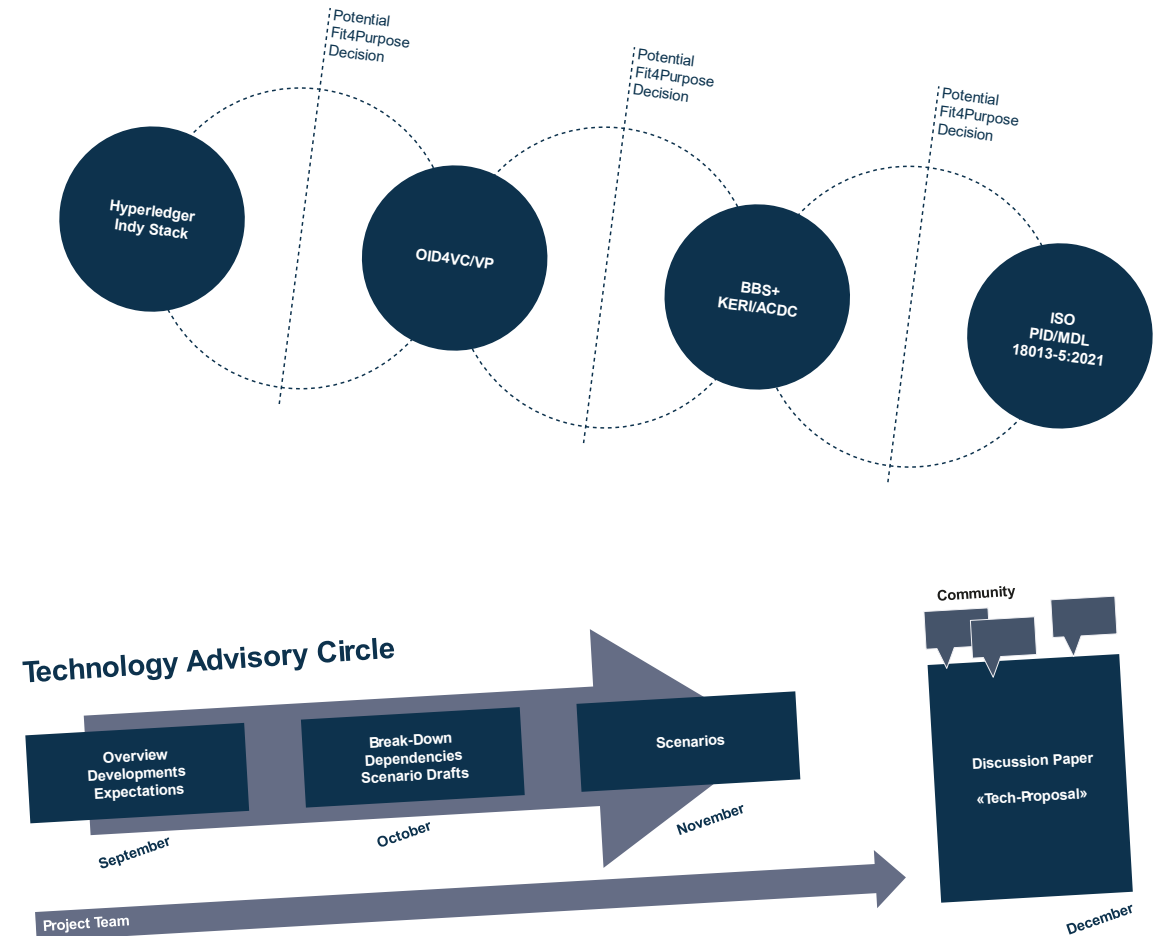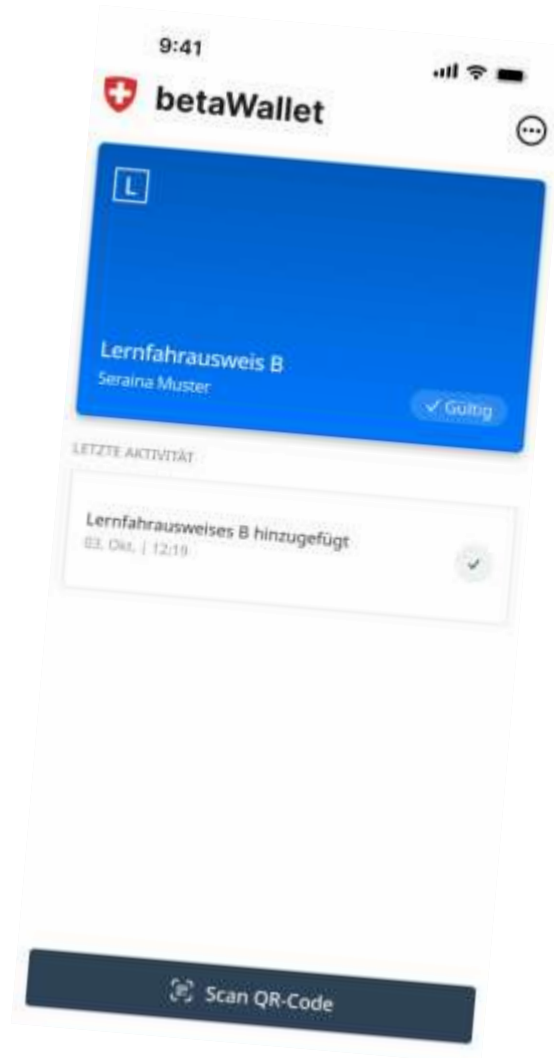**Zollikofen, 01.12.2023**

What are we talking about?

Defining common ground for the Swiss electronic identity and other verifiable credentials

How do we get there?

☑ Technical Advisory Circle

☑ Dedicated Tech-Spikes by E-ID Development Teams

☑ Hands-on experience by E-ID Development Teams

▶ **Public Consultation on Discussion Paper**

Hyperledger Indy Stack

OID4VC/VP

BBS+ KERI/ACDC

ISO PID/MDL 18013-5:2021

Potential Fit4Purpose Decision

Potential Fit4Purpose Decision

Potential Fit4Purpose Decision

Potential Fit4Purpose Decision

Technology Advisory Circle

Overview Developments Expectations

Break-Down Dependencies Scenario Drafts

Scenarios

Community

Discussion Paper «Tech-Proposal»

September

October

November

December

Project Team

Challenges in Technology Selection

A solution that covers all aspects has yet to establish itself **?**

Unlinkability

Technological Maturity

EU Inter-operability
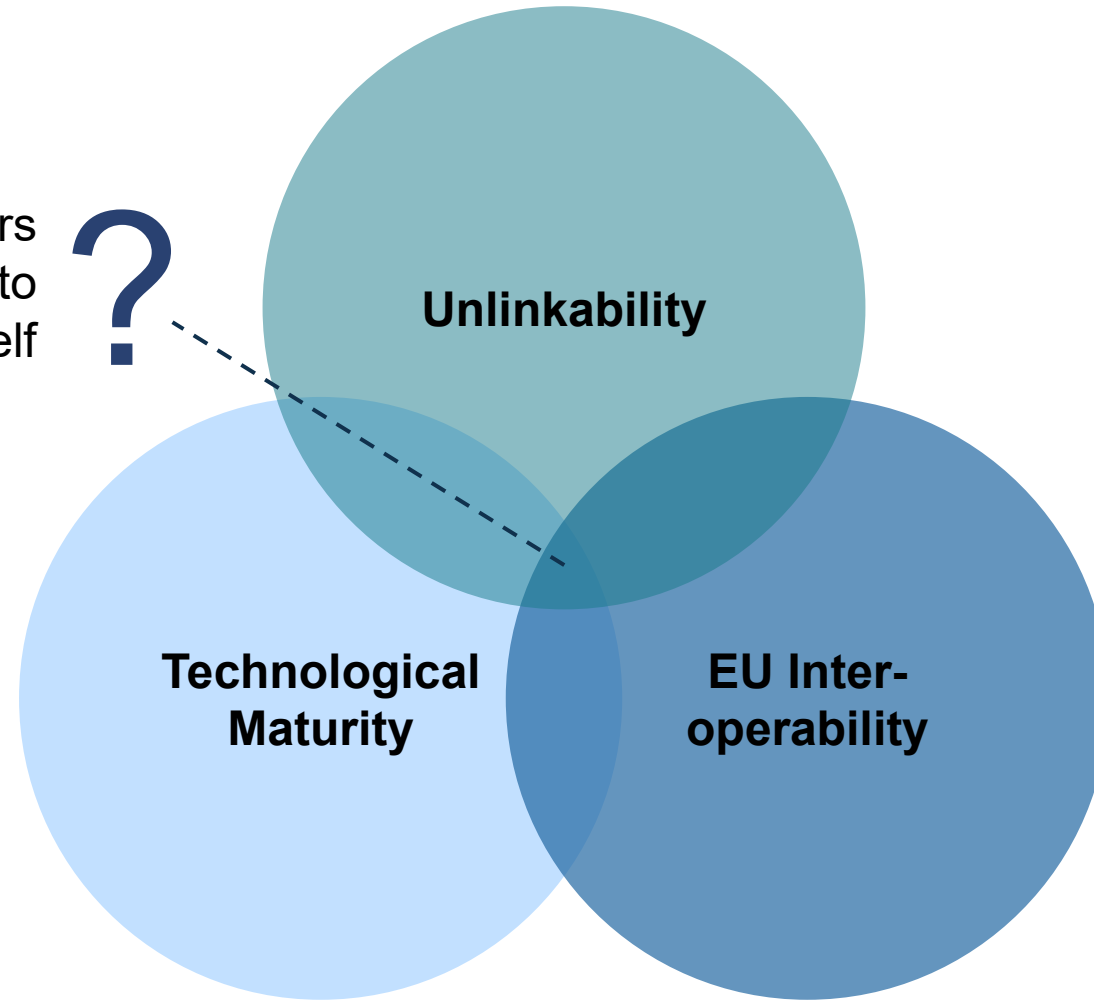
Discussion paper

The discussion paper covers these chapters

- Purpose of the document

- Background

- Design Principles and Criteria

- Decision on technological scenarios

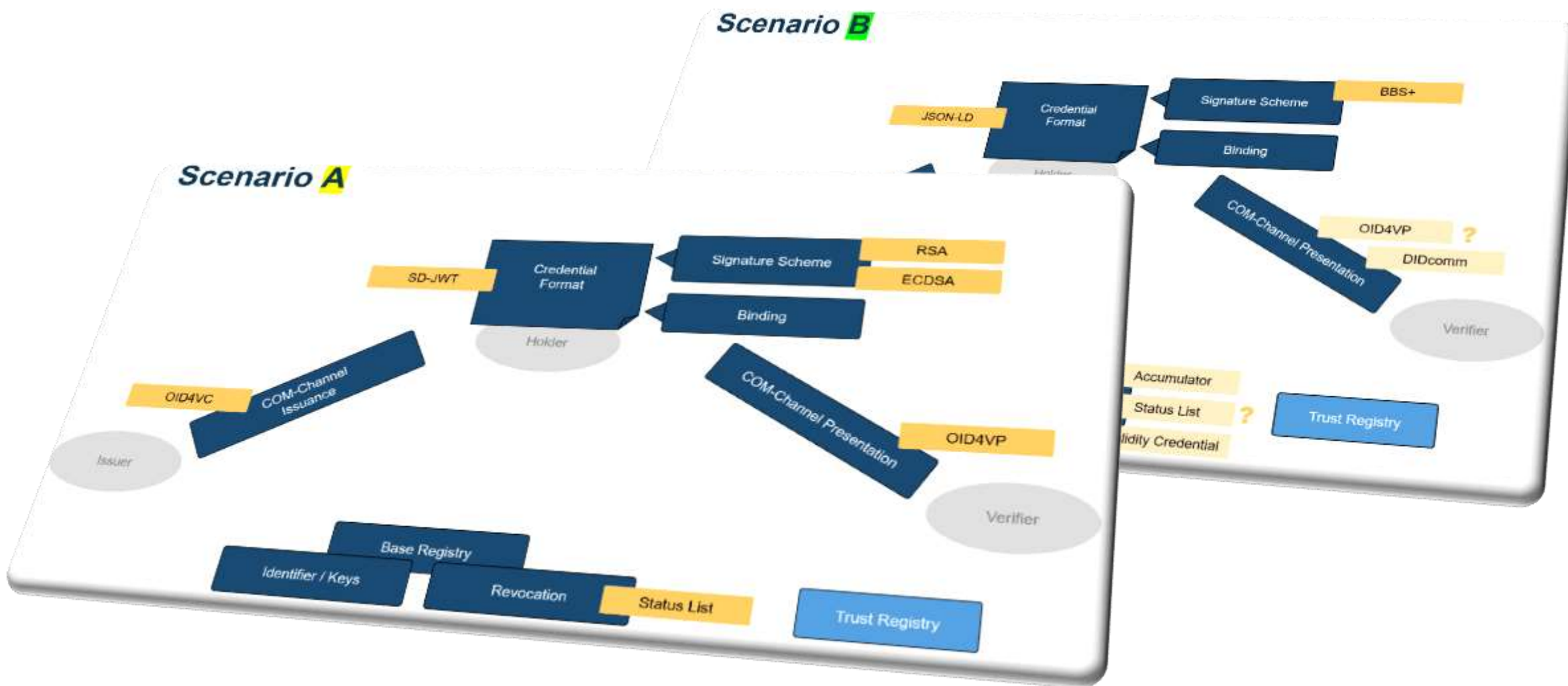- Public discussion of this paper and further process

- Annex

It is published on GitHub:
https://github.com/e-id-admin/open-source-community/tree/main/discussion-paper-tech-proposal

Scenarios

Scenarios

Scenario A

Main benefits for a Swiss Trust Ecosystem
- Potentially easier compatibility with the EU
- Common technology and standardised cryptography
- Easy understanding and integration for service providers
- Support for hardware-based cryptography

Main drawbacks for a Swiss Trust Ecosystem
- Potential linkability of the holder's credential use
- Potential traceability through revocation
- No predicates or zero knowledge proofs
- Selective disclosure is only achieved in a partially data saving manner

Scenario B

Main benefits for a Swiss Trust Ecosystem
- Unlinkability for holders is provided
- Correlation of holder data is made harder
- Selective disclosure is achieved in a data sparing manner
- Privacy preserving revocation might be achieved
- Zero knowledge proofs and predicate proofs seem attainable

Main drawbacks for a Swiss Trust Ecosystem
- Initially no technical compatibility or additional effort needed to reach interoperability with the current EU ARF
- More complex integration and less known cryptography
- Security of proposed Scenario less researched
- Smaller community

Positioning of proposed Scenarios

Subjective positioning by E-ID Team
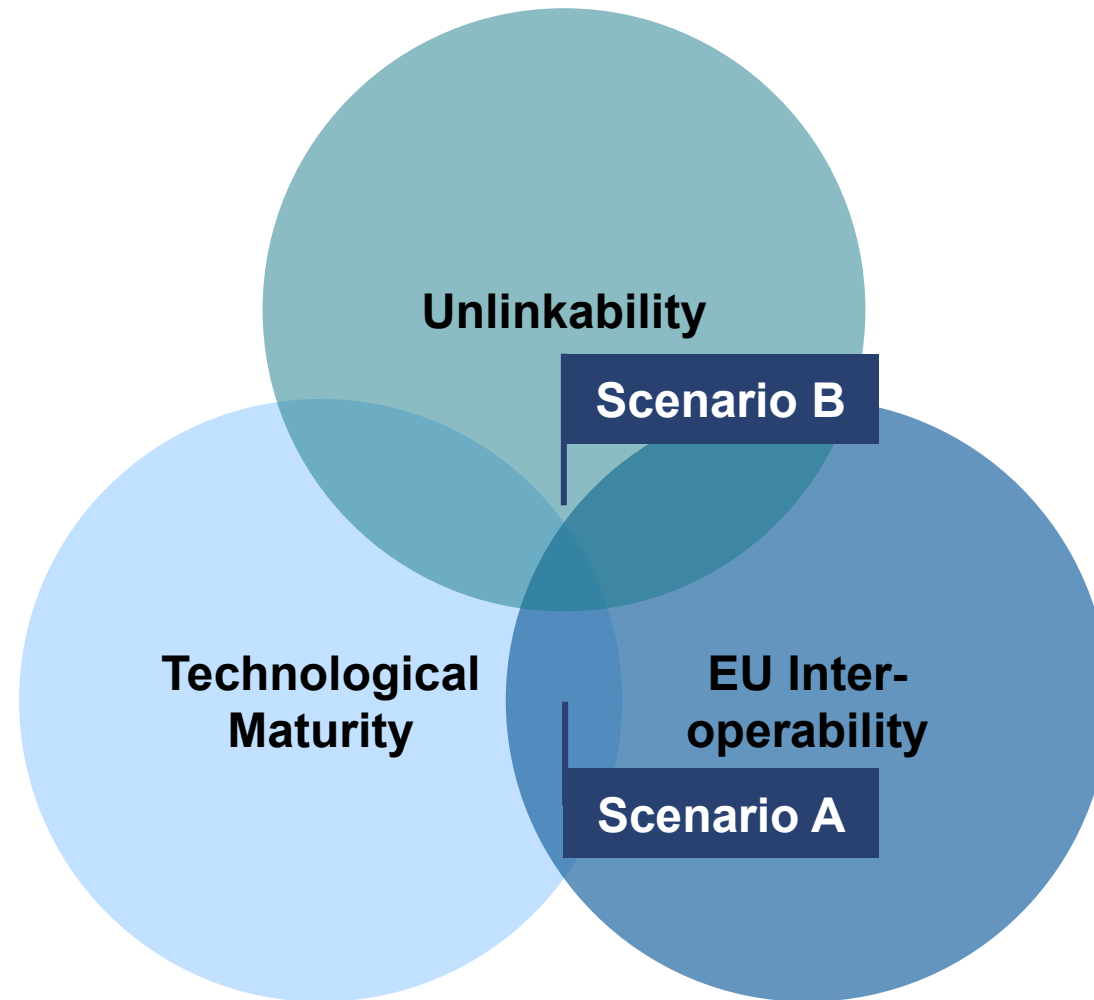
Public consultation on the discussion paper

Now your opinion is needed!

We are looking for answers to the following questions

- Which scenario would you prefer? And for what reason?

- Do both scenarios fulfil your expectations?

- What major risks do you foresee?

- Which "red lines" should not be crossed? Where is no compromise conceivable for you?

All responses will be published after the consultation period has expired, including indication of the official sender.
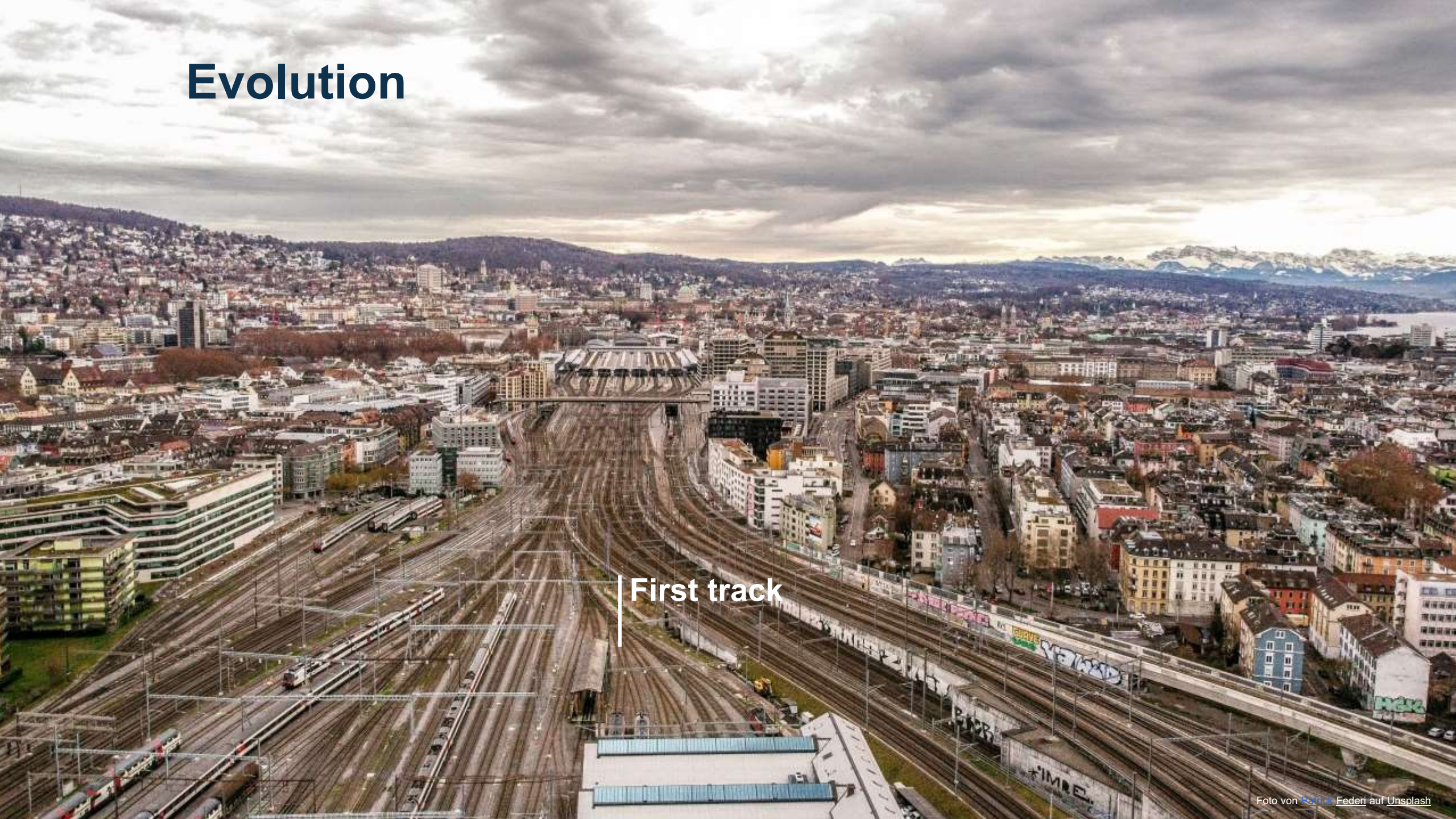
Consultation is open till **January 3, 2024**.

Link to «findmind»: https://findmind.ch/c/XFvu-a7c6

Evolution

First track