CH++

1) Which scenario would you prefer?

B[1]

2) For what reason do you prefer that scenario?

As a civil society organization, CH++ is deeply committed to data economy based on state-of-the-art science. Trust is central to the future eID ecosystem, and privacy by design is an essential tool to build and maintain this trust. The lack of data protection in the initial eID project was the primary reason for its rejection by Swiss voters (VOX, 2021), so the B scenario aligns more closely with their preferences. CH++ is also convinced that the compatibility of the Swiss eID with the future EU system is crucial. As has been shown with the Covid Proximity Tracing application, Switzerland can be a global forerunner, a solid Swiss solution developed and tested at pace has the potential to help set the standard.

At the same time, so much is unclear still in scenario A that there are certainly ways to build a good system on the basis of widely deployed cryptography — depending on the protocols and formats that process finally leads to.

3) Do both scenarios fulfill your expectations?

Yes

4) What major risks do you foresee?

Over-identification is the major risk we’re currently seeing.

Zero-knowledge proofs (ZKP) of knowledge as suggested in scenario B are currently mainly a theoretical concept with very limited real-life installations. This brings risks in terms of implementation and deployment. The fact that every wallet would have to implement it's own cryptography brings a lot of risk and uncertainty and also problems in view of post quantum resilience. As reference also serves the BSI opinion not supporting ZKP.

5) Which “red lines” should not be crossed? Where is no compromise conceivable for you?

-

[1] E-ID Tech Proposal: https://github.com/e-id-admin/open-source-community/blob/main/discussion-paper-tech-proposal/discussion-paper-tech-proposal.md