21.09.2023 - Meeting minutes #1 Technical Advisory Circle

Participants

- Christian Heimann (E-ID Team)
- Andreas Frey Sang (E-ID Team)
- Jonas Niestroj (E-ID Team)
- Tobias Bienz (E-ID Team)
- Christian Riesen (E-ID Team)
- Martin Burkhart
- Michael Doujak
- Damien Bowden
- Roland Riggenberg
- This Loepfe
- André Kudra
- Patrick Amrein
- Marco Dütsch
- David Berier
- Patrick Schaller
- Juraj Sarinay
- Georg Greve
- Michel Sahli
- Victor Martinez
- Vasily Suvorov
- Fabian Aggeler
- Christoph Graf
- Imad Aad

Notes

Introduction

Christian Heimann welcomes all participants and explains the working agreements and the ambitions of the technical advisory circle.

The main goal is to come to a common understanding and co-develop potential scenarios as a basis for the technical decision that the confederation will take. It is focused around the technical base of the trust infrastructure, which shall be the underlying technology used for the federal electronic identity as well as a national trust infrastructure. (P. 1,2)

The role of the other members of the E-ID-team, present in the call, is explained. They are mainly here to ask questions and listen to input from the community regarding the current state of play. (P. 3)

Thereafter, the “roadmap” for the technical advisory circle and the technical decision is presented. The goal of the first meeting is to kick off and gather an overview of current developments and expectations. In the second meeting, the idea is to further dive into requirements and dependencies, as well as come up with first drafts of potential scenarios. The third meeting, which will take place in November, will then focus on the detailed design and discussions regarding the aforementioned scenarios.

The output of this collaborative process shall be a discussion paper outlining the various scenarios and allowing a public discussion about what direction Switzerland might take regarding the proposed technical base of the future E-ID ecosystem. (P. 4)

The functionality of the technical advisory circle is explained, and the ambition to have at least two scenarios defined together is mentioned. (P. 5)

The discussion is then brought to some challenges facing a trust ecosystem in Switzerland today, especially regarding interoperability and the lack of a dominant design at the current time. As well as the various and sometimes contrary requirements raised by various actors. (P. 6)

The discussion is then opened and the community gets underway with various inputs. The following is an attempt to summarize the points raised by different members of the community. As discussed in the rules, there will be no attribution to a certain individual. Feedback and amendments by the participants is welcome and can be raised via GitHub. The points mentioned are individual opinions and do not constitute a consensus by the group (P. 7).

General discussion/comments:

- The requirements the federal government is faced with are challenging.
- It could be helpful to look at the data space to see what could carry over to the Swiss ecosystem.
- Adoption can also be a driver for a decision, so it could be helpful to analyze which SSI technology is gaining use in other domains (not necessarily related to identity), e.g., data spaces.

Regarding the European Union and the architecture reference framework for EU identity wallets

- The current discussions surrounding the EU Architecture Reference Framework / EBSI are considered a good start but are not considered a complete solution, and there is the expectation that certain aspects will need to be updated.
- Additionally, what is going on in the EU is interesting but will not necessarily happen in a time frame that is compatible with Switzerland's ambitions. As soon as eIDAS 2.0 is passed, approximately another 12 months will go by until the implementation acts are in force. The expected introduction of EIDAS 2.0 solutions in the member states is in about 36 months after the law has passed.

- In Germany, the Online Zugangsgesetz which provides access to digital services, is being pushed to use BundID. There is not necessarily any EU involvement in this.
- Being a bit more bold and taking independent decisions from the EU is advised.
- The political process in the EU is slow-going. The industry's adoption might preempt certain discussions.
- The ARF is considered to be too high level, further specifications will be required.

Interoperability

- International interoperability needs to be reached on three levels, on the semantic level, on the technological level as well as on the regulatory /legal/political level. In the semantic area, there are currently numerous initiatives ongoing. It also seems important to be able to issue credentials to holders in multiple format for interoperability (credential formats). Thus allowing them to hold to hold credentials in various formats verifiers might request. Technological interoperability might take more time to reach. The expectation of the community is that what is achieved now regarding semantics can be used or reused in the future, independent of technology.
- To be interoperable, it is advised to focus on multi-credential issuance. That ensures that the holders “at least” have the credential in the required format for presentation.
- Regarding the topic of interoperability, it is necessary to also focus on interoperability profiles within a specific tech stack, which define in more detail what aspects of the standards are used.
- It is advised to define an interoperability profile for Switzerland, use it with the community, test it, and then iterate on it.

SSI-Technology

- The phishing topic in SSI is mentioned as a problem. It is advised, that SSI not be used for authentication since it is not considered phishing-resistant. It is not considered an adequate replacement for passkeys or FIDO.
- The strategy of the EU lacks ambition, but it contains a lot of realism since it's based on easy-to-integrate technology and on cryptography that is known and scientifically researched.
- Given the lack of scientific research on zero knowledge proofs and unlinkability it is not advised to deploy this technology on a large scale.
- Additionally, the scientific background of BBS+ and Bulletproofs is questioned. It is unclear if these technologies are still at the level of white papers or if they are already in production.
- It is adviced to rely on technology which is known and has a successful track record.
- On the other hand, the experiments the federal government is doing with new technology is also considered good.
- Hyperledger is dying a slow but certain death. The specification is also considered to be suboptimal for broad state use.
- Instead of having a broad/open approach, it could also be beneficial to start with a very opinionated approach. Initially , only building blocks based on FIPS/NIST/ENISTA standards should be considered and a gap analysis should be made to identify requirements that can't be met. Only then should additional multi-format and multi-protocol approaches be considered.
- Regarding the topic of authentication and identity, it is agreed that there can be issues if one does not differentiate between the topics. A strong selling point is the movement of data between silos enabled by SSI.
- Additionally, it is mentioned that identity data is only one kind of data, which also has a high cost to verify. It could be advisable to start with other data.
- DID:WEB is considered to have the same benefits and pitfalls as the existing Web 2.0 (since it's rooted in the same technology).
- The project by the Frauenhofer Institute regarding trust registries via DNS is mentioned as a potential solution for certain requirements.
- The potential of KERI and ACDC is controversially discussed. The according white paper is considered quite hard to understand. Additionally, its community and/or authorship, which is small, is critically viewed. On the other hand, the cryptographic agility and the standard conforming cryptography are viewed as positive, as is GLEIF's ability to run it productively for their vLEI System. It is also being worked on by a community as part of the Trust over IP Foundation. KERI also contains the concept of key pre-rotation.

Stencil

The discussion is then moved to a stencil/blueprint to complete with technical elements, which is brainstormed with the community. The different actors /layers are discussed, and potential solutions to be analyzed per area are gathered (on the slideset P.8).

The discussion then covers the following topics:

Evaluation approach & comments on the stencil

- It is deemed helpful to have a sound criteria catalog for the different building blocks.
- The different technologies can then be evaluated objectively.
- It is also advised to adopt some architectural requirements that guide the decision process.
- The question is raised if existing infrastructure (Domain, PKI) can be used to achieve the goals of the project.
- It is advised to only use standardized cryptography in the crypto building blocks (e.g., CL-Signatures are not considered standardized/certified).
- The stencil is also considered to be a simplified depiction of the problem which needs to be solved. It does not display the complexity that is implied by multi-stack designs or by the interoperability with other ecosystems.
- It is advised that especially the wallets will need to support various standards.
- The Universal Resolver aspect is also not covered in the stencil.
- Additionally, the mDL-Stack is mentioned and the traction it is gaining in the United States.
- It is advised to adopt an approach that, regardless of which decision is taken, has an architecture in place which allows the ecosystem /infrastructure to upgrade and move on.
- Unlinkability is also mentioned as a risk since, in the event of misuse, the subject of the credential might not be able to detect misuse.

Next Steps

Christian Heimann then mentions that the next meeting of the TAC will take place on October 16th, 2023, from 15:00 to 17:00 (CET).

Additionally, the Hybrid Participation Meeting in December is mentioned, which will take place on December 1st, 2023, in Zollikofen at the FOITT.

The meeting minutes of the TAC will be released on GitHub and the discussions can continue there indepent of the meetings.