16.10.2023 - Meeting minutes #2 Technical Advisory Circle

Participants

- Christian Heimann (E-ID Team)
- Andreas Frey Sang (E-ID Team)
- Tobias Bienz (E-ID Team)
- Jonas Niestroj (E-ID Team)
- Christian Riesen (E-ID Team)
- Alexander Neumann
- Andreas Freitag
- Annett Laube
- Benjamin Rothenberger
- Blaz Solar
- Christoph Graf
- Damien Bowden
- David Berier
- David Sommer
- André Kudra
- Frank Michaud
- Georg Greve
- Helge Michael
- Imad Aad
- Juraj Sarinay
- Marco Dütsch
- Michael Doujak
- Michel Sahli
- Patrick Amrein
- Patrick Schaller
- Robin Pekerman
- Roland Ringgenberg
- Romain Poiffaut
- Sven Stucki
- This Loepfe
- Vasily Suvorov
- Victor Martinez

Notes

Introduction

The federal E-ID Team welcomes all participants and quickly recaps the group's working agreements and ambitions for the technical advisory circle.
The role of the representatives of the federal government is mentioned – they are mainly there to listen and benefit from the vast knowledge of the TAC participants.
A quick recap of the goals of the TAC and the current progress within the technology evaluation process is done.
Then the discussion paper is explained in a bit more detail, and it is clarified that the E-ID Team at the confederation will be the ones writing the paper.
The inputs of the TAC will be included. The names of the participants will be listed as participants in the meetings. (P1-P5).

Update IIW

The collaborative part of the meeting then starts with its first topic: updates from the IIW. (P. 6)

The impression of participants is that in previous years there had been many discussions about the differing standards (e.g., Didcomm vs. OID). The notion is that trends have changed in favor of OID and that DIDcomm was hardly mentioned. There was a lot of focus on the OID standard and defining interoperability profiles. It's mentioned that there are multiple interoperability profiles, which seem promising.

A further conclusion is that there are still few traces of trust list implementations and that there is still quite a lot of work to do to deliver the “full package” for a national trust ecosystem.

The work the OIX is doing is also deemed interesting since it mainly focuses on the aspects of governance and checking where there are current gaps. For instance, making trust lists compatible across multiple countries.

Google showed first APIs regarding Credentials. It's considered a first proposal, and they seem open to receiving change requests. Apple was not present at the conference.

The impression is that there are a lot more tangible solutions and products available based on the different strands of technology.

Keri was well presented by GLEIF and an issuance demonstration was available
There was a very high interest in KERI. For the community, its becoming more clear what it's advantages are and how to implement them.
A merge between ARF and KERI seems not thinkable at that moment.

It is mentioned that the EU Interoperability Profile is becoming more tangible.

The assessment is done that it seems realistic that there might be multiple solutions/SSI implementations that differ in their approaches:

- The EU solution, which is minimally invasive and easier for decision-makers.
- More radical approaches like KERI which touch on many different aspects. Which might not make it so easy to implement or to gain buy-in from decision-makers.

Nonetheless, it is worth mentioning that there is progress and further development in all the different approaches.

It seems there will be no unification of the different approaches in the near future. It's also worth mentioning that ledger-based solutions are not discussed to a great extent anymore.

The Hyperledger community is working towards did:webs. A more stable implementation of did:web. The government of British Columbia is also involved in this.
An important part of the community seems to have moved to other topics and stacks.

The interest in the OWF/TOIP has increased, and a lot of energy will be bundled there.
It will be interesting to see how the first collaborations in the code base go.

Discussion paper on the tech proposal

The federal E-ID Team presents the structure of the discussion paper, which will be published by the federal E-ID Team. (P. 7-8)
The goals of the discussion paper are mentioned.

It is stated that the scenarios contained in the paper will be worked on as part of the TAC. The lessons learned by the federal E-ID Team will also be integrated into the paper.

The timeline for authoring and publishing the paper is considered very ambitious by some participants. Due to these limitations it shall be come a short paper containing the necessary information for a broader discussion.

The question is raised if it would be possible to collaborate on the paper on GitHub. The federal E-ID Team refers to the structure already published on GitHub and requests that the community begin discussing important points or providing crucial information there. The early draft publication of the paper on GitHub for further collaboration will be discussed with the team writing it, and an answer will be provided at the next TAC.

A question is raised regarding the link between the proposed law and the discussion paper and how the current parliamentary process might influence the technological decision. It's discussed that the law aims to be as technology-agnostic as possible. There is an assessment that multiple technologies can fulfill the requirements prescribed by the law proposal.

Requirements

The federal E-ID then presents the basic requirements/principles stated in the publicly available draft of the law proposal and the six motions. (P.9)

A question is raised about what exactly is meant by privacy by design.
The assessment is that the requirement, as formulated on the slide, mainly means ensuring privacy in the sense, that issuers are not informed about holders actions.

There is a question about how a system can be decentralized if the confederation runs it.
It is acknowledged that the formulation on the slide is an oversimplification and that specific components of the infrastructure are meant by this (e.g., base registry, trust registry).

Regarding the topic of "overidentification", it is discussed that the existing Swiss Data Protection Act is in force and will also apply for the upcoming electronic identity and trust infrastructure.

There is a discussion about whether the law mentions what level of security or assurance is expected from the system. At the current time, there are no such requirements in the law. A Swiss level of assurance, conforming to “substantial,” is targeted. This is to enable use cases like opening an electronic patient record or simplifying the identification process to obtain the means for digital signatures.

The discussion then focuses on data privacy aspects, and it's mentioned that revocation schemes are relevant to the unlinkability of holders. Data minimization is also mentioned in the context of predicate proofs, e.g., is the subject of an E-ID older than 18?

The group then discusses the decentralized storage aspect. The law proposal leaves the decision on how to store credentials to the recipients. There might be certain requirements to conform to during the issuance process (e.g., holder binding). Nonetheless, it seems realistic that these requirements might be met by cloud wallets.

Regarding governance, it is mentioned that the requirements listed seem a bit short. It is deemed important to dive deeper into the requirements of the different sectors and see how governance can be delegated to authorities within those sectors.

There are also some risks associated with decentralized implementations. The secure storage of sensitive information is solely the responsibility of the holder. It's assessed that it might be hard for holders to detect stolen/lost credentials. In that case, verifiers might not be able to rely on the credential presented to them. These aspects might bring additional requirements for security.

Regarding data minimization, it is mentioned that this is not something new to the E-ID law, but that regulation has been in place since 1992, requiring the use of data in a sparse manner. It's added that ZKPs (zero knowledge proofs) might not be ready from the beginning, and that is deemed to be okay. What seems important is that the system has the capability to “grow” when technologies are available that allow more privacy-protecting use.

There are other voices that expect that verifiers will try to gain as much information as possible. It is questioned if technology can be the answer to these concerns, or if legal measures need to be in place. The FDPIC (Federal Data Protection and Information Commissioner) is mentioned as a potential actor to mitigate this.

Given the different terminology used in the discussion, it is deemed helpful if a normative reference/glossary is available.

Unlinkability

The TAC then focuses on the topic of "unlinkability". The federal E-ID Team explains that the fear of pending “overidentification” was a big topic in the public consultation. (P. 10)
While there are legal measures to address this, it is also desirable to assess the technical means available to mitigate the topic.

Some voices in the group mention that this can quickly become a political topic and that the role of TAC should stay focused on the technological aspects. It is mentioned that in the case of a security threat scenario, some countries might want to be able to actively correlate what a holder has been doing. Absolute unlinkability could therefore be perceived as a security threat.

It is mentioned that there is no law that, by default, requires the linkability of humans or their actions. Therefore, it is assessed that unlinkability should be a feature of the Swiss e-ID and not something that is given up easily.

There appears to be a consensus that there are plenty of aspects where linking can still occur (e.g., the content of the credential). There are currently no systems that comply with all aspects of unlinkability. Furthermore, context data already creates footprints. Some voices deem it hopeless to try to tackle this solely with technical measures. Laws that limit what other parties (other than the holder) are allowed to do or track are requested.

Unlinkability could be solved by legal measures. By focusing, for instance, on a "No E-ID obligation" by default, there would always be other means available to the user as well.

A participant mentions that this is something that should be “baked” into the system with no possibility of turning it off.

Other voices agree this is an essential feature, especially in light of ambition level 3. There might be other use cases or credentials that differ from the e-ID, where unlinkability becomes even more relevant.

BBS+ which is currently in an IETF standardization process, is mentioned as a possible solution for this topic. It offers plenty of benefits but seems not to contain range proofs at the current time.

Measures at the wallet level are also deemed helpful to alert the users.

Anonymous pseudonyms, either linked to the electronic identity or issued by the government, could be another solution that could be used.

An analysis of each use case is also deemed helpful. There might be different types or profiles based on the level of assurance to be reached: For instance, something based on the EUDI Wallet Profile 1 but with multiple issuances of the credentials. And a second profile based on W3C credentials using BBS+ for instance.

There are some further voices advocating not to throw it overboard by design. It should be tackled, but not all effort should go into the topic. Best practices for unlinkability should be implemented as advised by the technical community.

It is mentioned that the E-ID should not add another level that makes us even more linkable and traceable. If context is set by using the internet, there cannot be any improvment on privacy just by adding something. Nontheless there are various use cases where proof needs to be provided (e.g., age of minors) where it is not desirable to have a further data trace.

Criteria

The TAC then spends the remaining time discussing the criteria clusters listed by the federal E-ID Team (P. 11).

Post-Quantum

The use of post-quantum cryptography is discussed. There are some algorithms currently under standardization, and it's expected that this should have settled down by spring next year.
In the context of SSI, JSON LD-Proofs might be able to tackle this topic by being able to provide multiple signatures.
Given the ambitious timeline of the Swiss E-ID program, it seems like solutions need to be found that do not consider post-quantum cryptography to start with. Migration paths need to be considered.

Hardware backed keys

The question is raised if only signing algorithms are in scope that can be hardware backed.
The federal representatives explain that for issuing hardware backed keys are highly preferable and most likely a hard requirement - at least for government issued credentials. On the wallet side, there is the expectation, that technologies like the secure enclave/TEE will be used. It is assumed that mobile devices do not necessarily need to support the same signing algorithms as the VC's in order to establish a holder binding in the VC.

Revocation & Expiration

Revocation and expiration are mentioned as potential further criteria clusters, or at least as topics to be considered.
Especially regarding privacy preservation, there are challenges thatcould lead to problems if not tackled in an architectural manner.

Closing of meeting

Due to the advanced time, the slides regarding the stencil and the scenarios are skipped. They will be tackled in detail at the next TAC.
The federal E-ID Team thanks all participants. The next TAC will be on November 9th, from 3 p.m. -5 p.m..