09.11.2023 - Meeting minutes #3 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)
- Martin Burkhart (E-ID Team)
- Andreas Freitag
- Annett Laube
- Benjamin Rothenberger
- Bogdan Mocanu
- Christoph Graf
- Damien Bowden
- David Berier
- David Sommer
- André Kudra
- Frank Michaud
- Georg Greve
- Imad Aad
- Juraj Sarinay
- Michael Doujak
- Michel Sahli
- Patrick Schaller
- Robin Pekerman
- Roland Ringgenberg
- Romain Poiffaut
- Sven Stucki
- This Loepfe
- Vasily Suvorov
- Victor Martinez
- Vladimir Simjanoski
- Franziska Muschik

Notes

Introduction

The federal E-ID Team welcomes all participants and opens the floor asking the participants to share their news.

News from the participants

EU trilogue

The EU trilogue just finished, but the new legal text is not yet available to the public. It is recommended that the whole industry closely follows the process. An open letter has been published, which was signed by over 500 members of academia, civil society and data privacy organizations. It is suggested that participants read the letter and analyze the criticism raised in it.
The letter is available here.

Post Quantum

It has become clear that quantum computers will eventually break asymmetric encryption schemes. But there are different oppinions how fast this could happen.
Post quantum products are slowly becoming mature.Big infrastructure providers are preparing the ground today.
It was also pointet out that symmetric cryptography is not affected by quantum computers.

There is a lot of research currently ongoing and the first signature schemes are in the evaluation process to become certified.

If the new E-ID system will come out in 2025, it may need to move to post quantum signature schemes soon after. This implies that the E-ID needs to have a plan how to integrate postquantum signature schemes, as changing a signature scheme in a running system will be hard.
It was also mentioned that the currently evaluated quantum proof signature schemes will not support the privacy features promised by BBS+ or AnonCreds.

It is said that the topic must be regarded on different levels:

- transmission of data in a encrypted channel, that could be broken by post quantum products
- the signature of credential that could be falsified

Key parts that will require changing are CA certificates, roots of trust or migrating long-life credentials to post quantum and the participants believe that it will not be easy to do so.
Some participants understand that the term crypto agility includes this type of system change and the E-ID system needs to enable this change without losing functionality.

Others see that the internet will have to make this transition as well and that there is little use for the E-ID to switch, before the internet made this transition.

There will be a time where both algorithms have to be supported but if the old algorithms really become unsafe earlier than expected the old system has to be shut down.
A recommended approach is to go hybrid like google and Cloudflare. Only a part of the stack will need to be quantum proof. The two parts need to be independent so, if necessary, the non-quantum proof part can be shut down independently.

Secure elements

Secure elements in mobile phones are expected to play a key role in safeguarding private keys.
If private keys need to be copied from a secure storage in the cloud and transported to the user, some of the more serious public processes such as elections will not be doable through the E-ID.

Mobile phone providers will need to catch up with their hardware when considering the post quantum discussion. Renewal-lifecycle of hardware takes time. This time gap can lead to problems.
EU seems to have discussed the Usage of eSIM as Possibility for E-ID-Applets.

Prepared Technical Questions

News from topic “Interoperability Profiles”?

No comments from the group.

Holder-Binding for JSON-LD/BBS+: experiences?

There is academic research ongoing how the currently available papers suggest the implementation for credentials with JSON-LD/BBS+. So far, the finding is that the papers describing the cryptographic concept are not complete, especially around the topic of presentation and also certain terminology in the papers is not clearly defined and not used very consistently. Multi message signature scheme is well specified but the more advanced cases are not well researched yet.

It is stated that there is no difference BBS and BBS+.

BBS+ is still work in progress. It is claimed that there is a missing approval. To avoid getting in the same trap, direct anonymous attestation (DAA), a way to sign something without publishing the public key, is mentioned. There have been many failings in DAA to implement and might give some learnings for BBS+ implementation attempts. DAA implementation attempts had a large budget, specialized teams and dedicated hardware. Even with all these prerequisites it was difficult.

Holder-Binding is also possible in SD-JWT and is not particular to BBS+. The challenge is to do it in an privacy preserving manner. To achieve that it is advised to take a pragmatic approach rather than trying to achieve full privacy preservation and never getting anything into a production ready state. Also Germany discussed a long time to find the full privacy way, but tries today to get a much more pragmatic approach.

A way to do it in a privacy preserving way with SD-JWT is to use batch issuing. It will be a challenge to integrate this mitigation path in a user-friendly way. The approach to privacy needs to be pragmatic. Compared to a centralized system it's still a big improvement. BBS+ might just make the solution more complicated and not provide the solution it promises.

Revocation-check through verifier vs. non-revocation proof: Pros & Cons? Accumulator vs. StatusList?

It’s stated that accumulators need a call home function; are not scalable and mature for now. No productive accumulator implementation was known by the participants.

A product that has been using status lists for years are qualified signatures. For this use case there is no call home but can periodically request list and cash the data which can be searched. This works for qualified signatures as there are companies in the background that manage the signatures but for VCs this would not be the case and each VC would contain private data of the owner.

A third option for revocation proof is suggested other than accumulators and status lists. In the W3C specification there is the option to re-issue a credential with short lifespan. The downside is that the issuer needs to re-issue the whole credential. To each credential this can create a validity credential with the original issuing date. So, the system only needs to re-issue the validity credential. This does create a sort of call home, but it improves the situation where only the issuers need to be managed rather than both issuer and verifier. This would imply that systems also need governance rules for implementors so that malicious issuers can be avoided.

It is stated that validity credentials have too many downsides, as they effectively create a call back from holder to issuer. Another Option could be to use Online Certificate Status Protocols.
The upside of status list is that they are easy to roll out and scale with content delivery networks.

If a system does not have Zero-Knowledge-Proofs but has validity credentials the issuers need to work together to profile anybody, but if the system works with status lists the verifier can check the status of any previously verified VC at any time. It can be seen as a feature that a verifiable presentations validity can be checked over time to avoid re-presentation of the holder to the same verifier. But this aspect was also considered a privacy issue from other participants.

Bulk revocation of all credentials in a wallet in case of a stolen phone needs to be an researched.

Communication standards OID(4VC/4VP) vs. DIDcomm:
Matching the criteria of maturity, operational aspects, ease of implementation…?

The reusable connection offered by DIDcomm is very handy, and scalable. It needs a mailboxing on the side of the wallet, as this component is not constantly online.

It is reported that the topic of DIDcomm and the combination with OID was discussed at IIW and IDunion created a working group around the topic. Some members are of the opinion that DIDcomm might end up in the EUDI architecture reference framework eventually.

The trust over IP credential format comparison is mentioned as a useful overview.
And ToIP is evaluating different Protocols: https://trustoverip.org/blog/2023/10/10/simplifying-the-selection-process-for-credential-issuance-and-presentation-protocols/

The two channels have been built with different ideas in mind. OID is built with authentication and authorization in mind, built simpler and made easy. In addition for verifiers that already have OID connect they can easily add OID4VP, which could help scale the E-ID rollout. But it is also countered, that to switch from OIDC to OID4VC isn't that easy; payloads are different, only the flows are similar. DIDcomm is good for asynchronous communication, is transport agnostic and has better cryptography options than OID. If a system wants to use DIDcomm it needs to be able to use DIDs.

It is stated that it depends on the use case which method is more suitable. For the E-ID it could be beneficial to use a multiprotocol approach with wallet discoverability depending on the protocol the wallets use, issuers have the ability to use both and adjust depending on what the wallet is able to do. To discover what the wallet can, the issuer checks the DID document where it states what it can do.

Ideally DIDcomm will end up in a trust spanning layer that goes far beyond Credentials.

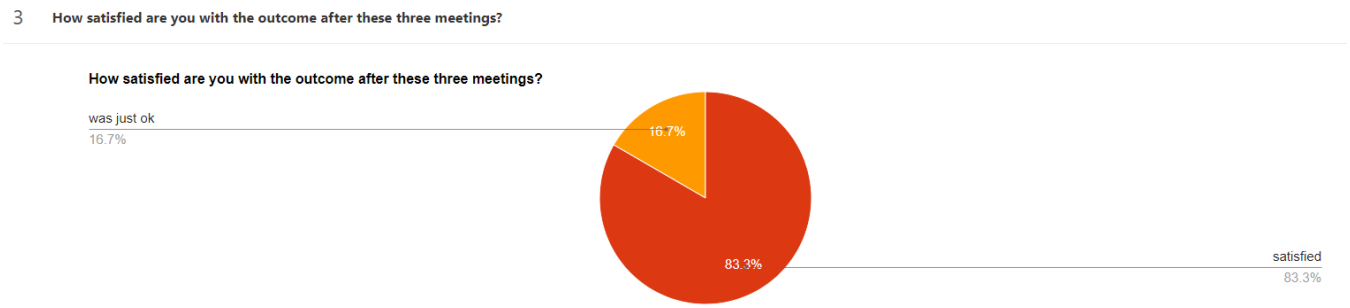
Discussion Paper «Tech-Proposal»:

The E-ID team shows the roadmap for the discussion paper and where to find the publication and invite to check the draft from Nov 13, 2023.

Survey

Small survey about the passed three TAC meetings. 12 participants answered the survey.

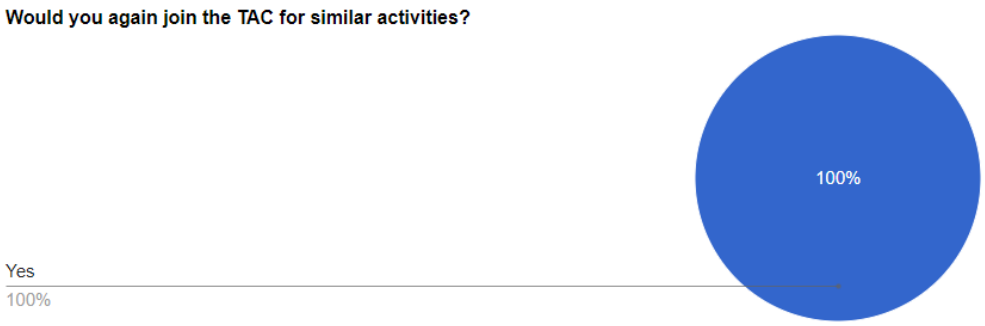
Results:



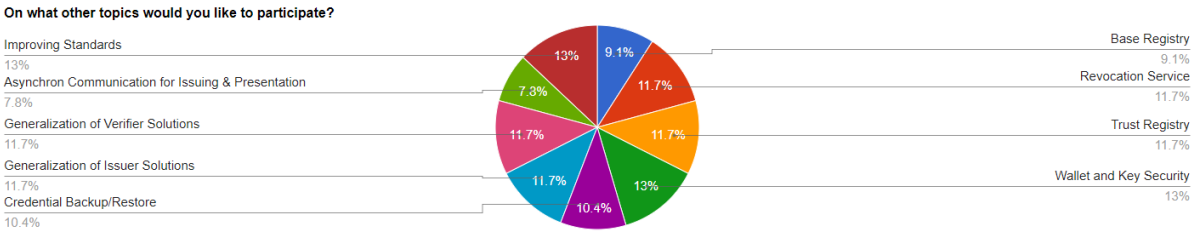
4 What should the E-ID Team do better next time?

Teilnehmer	1 -
7997183	Preparation time should be longer
7997368	Send content of TAC earlier.
7998540	Not much more, hard position and there was a good communication management during the circles
7998546	The E-ID Team did good overall. Maybe it could have been of value to include more larger private sector representatives to foster future adoption, by aligning early on.
7998547	The team did a great job! Always being prepared and having a clear guiding and facilitation approach gave the attendees a lot of space to have valuable discussions. As you ask specifically about what to do better, I'd say 5 instead of 3 installments. But I guess managing the 3 already was a lot of work. Well done!
7998548	Evtl. wäre es einfacher über einen bestehenden Draft vom Dokument zu diskutieren, was bei der kurzen Timeline aber wahrscheinlich nicht möglich war.
7998552	Limit the scope of topics
7998553	Probably make the meeting on-site
7998555	nothing, there are just too many topics we have not covered yet. keep up the good work
7998563	I'd appreciate to learn more about the people on the TAC. It's positively self-guiding to some extent as people declare their field of expertise and/or why they feel they have deep/rich insisghts worth sharing. Assembly of the circle might be something that interested parties outside the TAC would be keen on knowing.

5 Would you again join the TAC for similar activities?



6 **On what other topics would you like to participate?**



Diagrammtyp Diagrammgrösse

Option	Prozent	Anzahl
Base Registry	9.09%	7
Revocation Service	11.69%	9
Trust Registry	11.69%	9
Wallet and Key Security	12.99%	10
Credential Backup/Restore	10.39%	8
Generalization of Issuer Solutions	11.69%	9
Generalization of Verifier Solutions	11.69%	9
Asynchron Communication for Issuing & Presentation	7.79%	6
Improving Standards	12.99%	10
12 Teilnehmer	**100%**	**77**

Closing of meeting

Invitation to the next public participation meeting.
The E-ID Team is grateful for all the efforts and inputs given by all the participants.