Call for Ideas

This page collects proposals for future Incubator activities. Anyone may add a new idea by adding a new row to the table below.

Ideas don’t need to be fully formed but the more scope we can get the easier it will be to assess whether the idea should be taken forward.

Anything in the Trust and Identity space is of interest, from improvements to current services to brand new ideas and technologies.

If you like an existing idea you can just add a +1 for endorsement. The more supporters a proposal gets the more likely it is to be implemented.

### Example from a previous cycle

<table>
<thead>
<tr>
<th>Title</th>
<th>Proposer</th>
<th>Description</th>
<th>Supporter (+1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Self service - Signin</td>
<td>Janusz Ulanowski (HEAnet CLG)</td>
<td>Service which could allow an user to check signing in activity on IdP service. That would allow an user to check the recent activity on his account in regards of authentication. Users could see the list if authentications containing datetime, ip and relying party etc. That would help them to spot suspicious activity.</td>
<td>Janos Mohacsi: it would be advantageous to have a standardised log format to all popular IdPs. Then these logs should be dumped to ELK or similar server. The log collection server should provide a restricted access to the logs of a particular users. Mihály Héder: I think an Audit Log self-service is an interesting functionality. Account activity is available in many commercial accounts, certainly the googles and the microsots of the world. We should keep up - also not only the IdP Audit Log but the SP is relevant.</td>
</tr>
<tr>
<td>activity</td>
<td></td>
<td>After discussion in the Incubator board, the proposal for the Incubator is inspired by the above proposal, but with a slight difference: Setting up a service as proposed originally is rather challenging as that service would have to learn about a lot of personal data. However, ‘account activity’, deployed as part of an IdP extension would actually improve privacy and GDPR compliance of e.g. SimpleSamlPHP and Shibboleth. Proposal is to create such extensions for SSP and Shibboleth in close collaboration with the relevant community Both SimpleSamlPHP and Shibboleth as well as also support the OIDC protocol. A profile page should also allow an end user to manage and revoke OIDC access.</td>
<td></td>
</tr>
</tbody>
</table>

### Proposals:

- Investigate Google WEI & Apple Private Access Tokens
- Scalable, interoperable revocation
- Passkey registration to User Profile Page (Shibboleth)

### Proposal details:

**Topic submission deadline**

The Call for Ideas for for cycle 8 (Apr 24 - Dec 24) is open.

The submission deadline for the next cycle is 15 March 24.
Investigate Google WEI & Apple Private Access Tokens

Mihály Héder (KIFÜ /SZTAKI)

Google Web Environment Integrity is a method for websites to verify that the client platform (User Agent a.k.a. browser + operating system) is indeed genuine and has not been "tampered with": https://github.com/RupertBenWiser/Web-Environment-Integrity/blob/main/explainer.md

The protocol relies on integrity attestations.

The proposal has received strong criticism, the interlocutors mostly claim that it is just a harmful way of achieving DRM. For a summary, see the Wikipedia entry: https://en.wikipedia.org/wiki/Web_Environment_Integrity

The insight of the CEO of Vivaldi browser is especially interesting: they apparently already need to spoof the user agent string in order to be able to use Google Docs, despite the fact that Vivaldi is based on chromium. https://www.theregister.com/2023/07/27/google_web_environment_integrity/

By the proposers it is purported to be a replacement of browser fingerprint-based anti abuse methods. https://github.com/RupertBenWiser/Web-Environment-Integrity/issues/28#issuecomment-1651129388

They also claim that it is a better alternative than Apple’s Similar Private Access tokens, another attestation scheme that works between Apple devices and Cloudflare. They also claim in defense of WEI that they may help sunsetting the increasingly useless CAPTCHAs.

WEI is already supported by Chrome on Android.

It could turn out to be crucial that our community understands these protocols and develop its own relationship to them. Also, while the attestation about personal devices seems indeed quite privacy-endangering as well as the prospect of enhanced DRM, there may be legit use cases for classroom devices or around the integrity of wallets.

The proposal is to explore, try out WEI and write a report for the community. Perhaps the timing of this proposed activity is also a strategic concern - if the WEI proposal will have no good reception then there is no point in wasting resources on it, but if it there is uptake then we should react.

Janos Mohacsi (KIFÜ)

Scalable, interoperable revocation

Stefan Liström (SUNET)

Revocation is not only a mandatory privacy enhancing feature for endusers, it is also a core security feature. Both use cases for revocation need to be implemented in a future EUDI wallet ecosystem. There is currently however no clear solution for interoperable, scalable revocation in the EUDI. This activity investigates and describes the possible approaches for scalable, interoperable ways to handle revocation. The activity should try to test at least two of the approaches with respect to requirements on scalability and interoperability as may needed for the EUDI.

Passkey registration to User Profile Page (Shibboleth)

Janne Lauros (CSC)

This proposal is continuation to earlier incubator work where User Profile Page for Shibboleth was implemented as means for the user to view the available user data and the tokens issued on behalf of user (https://github.com/GEANT/shib-idp-profile).

Shibboleth project is working on WebAuthn authentication flow and has define the scope for the Passkey management as "The inbuilt flow represents the minimum viable product for implementing such a feature. In the future other plugins may provide this functionality".

We propose following task for the next Incubator Cycle to provide additional features for Passkey management

- Add Passkey registration to UserProfile. Work should be done in cooperation with Shibboleth team to guarantee best integration to interfaces provided by Shibboleth project.
- The user must be able to register and manage multiple Passkey credentials.
- An optional API providing organization tools to list and remove Passkeys of users.
- An optional administrative function to allow an administrator to define requirements for authenticators (via Attestation).