Engagement with W3C FedID CG

Through W3C TPAC in Sept 2023

We’ve been following the working group charter drafting and have submitted changes that we intend should take into account authentication proxying and current SAML capabilities. W3C membership will be needed in the working group to ensure attention is paid to these issues.


April 2023

Moving to proposals directly in the proposal repository

March- April 2023

After the hackathon, the REFEDS Browser Changes working group took over scheduling meetings for our community, trying to keep up with the weekly cadence of the FedID CG meetings. Moving these proposals forward with the FedID CG is harder without the deep discussions we had at the hackathon. We continue to engage, and are moving forward with refinement of the proposal and the communication.

- **Idp-sp-storage-api aka ISSUE 4**
  - https://docs.google.com/document/d/1UWuw9_9EAnwtsct9K6j7BN_ybcMSs2p00xbo9U9O1s/edit?usp=sharing
- **Offloading Trust: aka ISSUE 5**
  - https://docs.google.com/document/d/13eFqvyQ6VdRh13IjILAL9YUUJd_0S2ej5ixiU0ImQ0/edit?usp=sharing

Dec 2022-March 2023

At the 45th Meeting of REFEDS (Monday, 5th December 2022 as part of the 2022 Internet2 Technology Exchange) Heather Flanagan gave a presentation on “The browser privacy changes and what it means for R&E federations (update)” (pptx) and then she provided a broader overview with a Techex22 presentation “The Web is for Everyone, Sort Of” (pdf). While there have been previous discussions within the R&E Federation community about this work, these two presentations had a clear message:

“The changes in the browsers are coming; other communities have tried to stop the changes but it hasn’t worked. There’s an opportunity to work with the W3C on these changes but the window of influence is closing.”

At ACAMP in the days following, attendees discussed what our next steps would be in addressing these changes. Some of the ACAMP sessions included Seamless Access FedCM (Wallet?), Art of raising awareness digital wallets, FedCM, and – before ACAMP was over – we began FedCM Hackathon Planning (replacing Discovery) and how to do this with SSP, idPy, Shib (links go to session scribing documents). REFEDS 2023 work planning was in progress, so we proposed the “Browser Changes” Working Group (REFEDS wiki).

Since then, a group used the REFEDS Slack and a few meetings to prepare for a two day summit with representatives from the Chrome and Firefox browser teams in Mountain View, California at the end of February. We spent some time understanding the FedCM specification as it stood at that time.

At a high level, the W3C FedID group has two current goals: the explicit goal is to ensure that the user consents to the RP and IdP exchanging information before exchanging information with the two systems. In the consumer authentication world, there’s a privacy issue of the IdP being aware that the consumer is logging in to specific RPs. The urgency is driven by consumer IdPs that have user experience “improvements” that depend on third party cookies. The W3C is taking tracking issues in the browser seriously, and is pursuing methods to make tracking much harder, with the limitation of support for third party cookies – which are extensively used in tracking – in progress.

When we gathered, we explained the R&E Federation trust models, enforcement actions, and needs. We felt that the two representatives really saw and understood the strong trust model of multilateral federations. With a great deal of enthusiasm we put together two proposals that we brought back to the W3C Federated Identity Community group (FedID CG).

Issues to raise

- Issue: Missing support for when isLoggedIn is not set
- Issue - multiple IdPs: IsLoggedIn state may hide the option to log in with a preferred IdP
- Issue - multiple IdPs: the user-client calls to IdPs must scale for a user having access to multiple IdPs
- Issue - multiple IdPs: User-agents must be required to respect RP’s offer of multiple IdPs
- Issue-proxies: Browser agents must provide full browser capabilities when presenting a session restoration method
- Issue-proxies: Missing support for authorization intermediaries
- Non-issue: the .well-known file