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).

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.

We are also chartered with helping the wider R&E Federation community and all the organizations that may be impacted to become aware of the changes in progress. The immediate issue of third party cookies being blocked by browsers is not a significant issue for the existing authentication flows. It has impacted some of the elegance of Seamless Access’ simplification and persistence of the discovery process. However, there are tracking techniques called bounce tracking that are, from a browser’s point of view, indistinguishable from federated single sign on. When browsers begin to mitigate against those tracking techniques, SAML protocol will be interrupted.

It’s unclear what the timeline may be for browsers to interrupt cross-origin redirects and POSTs. We engage now so that we can mitigate the possible impacts, educating the browser architects in how the web primitives are integrated in complex ways to create the trust fabric that supports learning and work and health care delivery across the web.