State of FedCM and SAML

As browsers turn off third party cookies, SAML and OpenID Connect protocols remain functional. The concern is that more aggressive techniques will be implemented in browsers to minimize the cross-site (eTLD+1) transfer of information about users.

Our concern is raised when the browsers take on navigational tracking with more force than the current plan. (Judith Bush TBD document Navigational tracking proposal.) When cross-site or cross-origin HTTPS redirects or POSTs come under more scrutiny, we hope that we can use FedCM or some version of it to signal that our protocols should be trusted across sites and origins.

Proposed usage of FedCM to protect protocols

In the April 2023 IIW side meeting, the REFEDS Working group members in attendance worked with the W3C CG representatives in attendance to outline a possible signal using FedCM as it stands to protect authentication protocols from browser identification of them as tracking. A working solution would be for an SP, prior to initiating a protocol flow, to use FedCM to establish user-to-browser consent. The SP would initiate the flow to the IdP, the IdP would respond that there is an account available (this would be the same account for any request). The browser would ask the user for consent, and if consented, would present the IdP with the SP client ID (SAML entity ID). At this point the IdP determines whether it trusts the SP. If it does, the "opaque token" that the IdP returns could be a constant value, essentially signaling that FedCM is satisfied and SAML can begin.

The participants acknowledge that this flow suffers when there are multiple cross-site hops in the authentication flow. Work for REFEDS is to advocate for improved

Points of consideration

IdP discovery and preference for IdPs

As yet poorly understood is whether FedCM will provide any assistance with discovery or persistence of preference for IdPs.

Site and origin trust vs entity trust

Early versions of the FedCM API identified the SP and IdP to each other at the origin level. As of the 2023-05-30 draft, the SP identifies an IdP by its configuration URL and provides its clientID as appropriate for the IDP. The user's consent is recorded at the origin level.

Each user agent has a global connected accounts set, an initially empty ordered set. Its items are triples of the form (rp, idp, account) where rp is the origin of the RP, idp is the origin of the IDP, and account is a string representing an account identifier. It represents the set of triples such that the user has used FedCM to login to the rp via the idp account.

Conceptually, SAML trusts entities and could have more than one distinct entity at the same origin. With the origins recorded as the point of trust, the browser consent may be broader than the federated trust.

The best example of SPs at the same origin so far is connect.liblynx.com which is associated with on the order of 10 different publishers. Liblynx is a cloud provider, the publishers all have independent relationships. The problem with it as an example is that publishers have their own domains -- if fedCM was used the domain would be the publisher's not liblynx. And at least the first two share the same encryption key. It would be GREAT to find something like liblynx but where the different tenants don't share the same key and go ahead and use the origin of the hosting platform. admin.floundry.net/ has around 22 different entities, also sharing the same key. What I don't know is if the actual usage is at pages with branded domains, and if fedCM was used the domain would distinguish.

Browsers do have a point in distinguishing trust at the origin level, perhaps even the site level, given that a cookie can transfer information across those boundaries.