FedID CG Telecon, 17 September 2021

- Moderator: Heather Flanagan
- Scribe: Tim, Lee

Call-in details: see https://lists.w3.org/Archives/Member/internal-fed-id/2021Aug/0000.html
Charter: https://github.com/w3c/fedidcg

Agenda

Administrivia

- Scribe volunteer(s)?
    -
- Reminders:
    - Community Group Membership
    - W3C Code of Ethics and Professional Conduct
- Slack link: https://join.slack.com/t/w3ccommunity/shared_invite/zt-tsegkiat-0jFvovmYG1KuK_MbmKVNHA
- Report from EIC?
- IIW?

Terminology Explainer (Draft Wiki page)

User Stories - Sanctioned vs Unsanctioned Tracking (GitHub template)

Any Other Business

General Library of Useful Reading

- 20 August 2021 fedidcg Meeting Notes
- Unsanctioned Web Tracking
- Tracking Preference Expression
- W3C TAG Ethical Web Principles
- Self-Review Questionnaire: Security and Privacy
- Web Platform Design Principles

Notes

Heather -- Recap of last meeting. Terms sanctioned / unsanctioned clarifications. Make sure we have a common understanding of the terminology so all proposals have the same meaning. We tried previously to get some set of cases which are 'obviously' sanction tracking vs obviously unsanctioned (this is in User Stories)

George -- Is IDP wanting to know about user information (including device information) during flows 'obviously sanctioned'.

Heather -- Using identity information for anything else outside of IDP is not 'obviously sanctioned'. Sam has been working on WebID proposal (link in Slack channel).

Sam -- Intention is to bring WebID proposal to the Group. Easy to fall into premature generalization (for (un)sanctioned). We should pick a couple of scenarios and talk more deeply to find patterns. We should break things down between privacy and security. We should use terms like "for security purposes". Then should discuss privacy separately, ie "what is the worst that could happen with the IDP having this information". Assertion is that usually they don't conflict. When they do conflict ... that is when more discussion is needed (example is SPAM / Abuse ... the more the IDP knows, the better it can work but it also has to gather a lot of data). When porting Privacy Threat Model, found lots of common terminology to use.

Kris -- Comments on WebID -- (1) IDPs / RPs owned by the same entity and potentially colluding. Response was that first party sets says this is 'okay'. Can IDP and RP from same entity not use first party set. Privacy should involve users being informed and choosing to

engage in certain behaviors. Shouldn't just be "done in the background' (users must 'understand'). Concern is how to educate (vs how to stop)

Sam -- 100% agreement around discussion on collusion. Must be part of threat model.

Kris -- Should call out the difference between collusion between different companies vs a single company that owns both IDP & RP where they might not even realize they are 'colluding'.

George -- Likes classification of business / protocol use cases. In <>, no data about the user is transferred and information is only passed via back channel. The requirement says that the UserAgent is *not allowed* to see the data so it must be backchannel. So there is a discussion to be had on technical vs legal.

Judith -- Does licensed equate to 'owned' with regards to relationship between IDP and RP.

Kris -- Was more thinking truly 'owned' but that is a good thing to call out.

Heather -- I see WebID taking new primitives (FPS) as a mechanism to prototype how to get FedID to work. When we have privacy concerns about FPS, we need to make sure we also bring them up in PrivacyCG.

Adrian -- How many people on this call are planning on having a product bought customers, ie Apple requires consumers be okay with what they are providing vs just Enterprise customers. If you don't have direct-to-consumer paths, unlikely to do a complete job on the security flows

Kris -- We have B2C and we are a SAAS provider. Very different considerations for B2C vs B2B. What people consider private is often very different.

Tim -- Google, MSFT, Ping, ... significant set of consumer IDPs on the call

Ken -- This started as consumer focused initiative. More worried that we miss the privacy rules associated with business rules.

Sam (in response to 'what feedback are you looking for) -- (Repeat) Make sure we are using the same terms and have the same meanings. Take small steps, establish first principles.

Use cases, threat models … foundational work to get agreement on. Example in threat model is passing global ids around. Can we go through that concretely as a group to talk through and get it polished. Work through the examples and figure out if we can classify as ‘sanctioned’ / ‘unsanctioned’ and start with easier examples like collusion. Thinking about Privacy exclusively is helpful

James -- Developing a use case for how to avoid sharing personal information but still get personalized preferences and how they can be informed and consent. Agree on needing to get agreement on the terminology cause they can be different for different cases / perspectives

Heather -- Opening issues on terminology is a helpful way to drive discussion / consensus. Pulling in Christos to talk about international education space

Christos -- The way we (education) use Federation seems to be very different then how everyone else seems to. Working with EU program (Erasmus) on full digitization of student records. As students move from school to school, go and come back, want records to flow correctly and so need to identify the user (student) uniquely in a way that will follow them throughout the student education lifecycle <?>. Currently 5000 universities. Also considering what to do with the research collaboration use case that brings together researchers around the world that require sharing resources. These collaborations range from tens to thousands, and open questions of incident response, tracking for collaboration, etc.

Beri -- Product lead on Google Web Platform. Thinking about future proof and backwards compatible. How can ‘we’ leverage the expertise in the ‘room’. Might have questions that span EU / Consumer / … how to reach out.

Heather -- you can always use the slack channel. You can also reach out directly or even setup a call if need be. We could spend the rest of our natural lives discussing terminology. What I am hoping … focus on terminology until Oct 4th (line in sand) and then focus should be on proposals and discussing them. And also putting together federation reviews of technology proposals (like FPS … as a building block, does that work for us, is it lacking, …). Can these building blocks work for federation.

Queue - add yourself at the bottom

-

Attendees (sign yourself in):

- Anthony Nadalin
- George Fletcher (Yahoo Inc.)
- Hirsch Singhal (Microsoft)
- Daniela Pöhn (Universität der Bundeswehr München)
- Emily Lauber (Microsoft)
- Tim Cappalli (Microsoft Identity)
- Lee Graber (Tableau/Salesforce)
- Kris Chapman (Salesforce)
- Brian Campbell (Ping)
- Allan Spiegel (Adobe)
- Andi Hindle (independent)
- Judith Bush (OCLC)
- Michael Knowles (Google)
- John Bradley (Yubico)
- Bill Densmore (ITEGA.ORG)
- James Rosewell (51Degrees)
- Kaustubha Govind (Google Chrome)
- Kaan Icer (Google Web Platform)
- Brittany Dungan (Google Web Platform)
- Yi Gu (Google)
- Christian Biesinger (Google Web Platform)
- James Hartig (Admiral)
- Beri Lee (Google Web Platform)
- Adrian Gropper
- Bjorn Helm
- Dick Hardt
- Janak Amarasena
- Kristina Yasuda (Microsoft)
- Sander Engelberts (OCLC)
- Ken Buchanan (Google)

- Sam Goto (Google)