




# Federation and Browsers

WICG WebID Workshop  
25-26 May 2021



# Administrivia

Are you a member of the W3C WICG?

Do you accept the W3C Code of Ethics and Professional Conduct?

Are you aware of the W3C Patent Policy?

Then welcome!

# Considerations for the workshop

Participants represent a variety of organizations and a wealth of sectors.

Each person has a different perspective on the problems of user privacy as balanced against SSO and federation over the web.

Workshop Goal: Participants leave this meeting with an awareness of the existence of the others and an understanding of the impact of not coming together to solve the problem.

Bonus Prize: We develop a concrete plan about how to keep all interested parties informed and engaged.

# Meeting management

- Use the queue in the notes document
- Please mute your line when not speaking
- Be prepared to be kept to time
- Volunteers for scribing?

*There are many additional topics that we wanted to cover (considerations around research & education, impact on protocols, use cases of a variety of RPs) but we only have so much time.*

# Thoughts on Day One

Positive outcome:

- Group made solid steps towards increasing awareness

Negative outcome:

- Highlighted (and possibly fed) a divide in willingness to work towards a solution

# Agenda - Day One

- Recap of Day One and Intro to Day Two (10:00 - 10:10)
- Problems and Solutions from the Browser Perspective (20min each)
  - Mozilla Firefox (10:10 - 10:30)
  - Microsoft Edge (10:30 - 10:50)
  - Google Chrome (10:50 - 11:10)
- BREAK (11:10 - 11:25)
- Identity Provider use cases (20min each)
  - Microsoft Identity (11:25 - 11:45)
  - Facebook (11:45 - 12:05)
  - Google Sign-in (12:05 - 12:20)
- BREAK (12:20-12:30)
- Wrap Up Day One (12:30 - 13:00)
  - Consider the questions for Day Two

# Submitting and Voting on Questions

## ***Day One Only***

So many possibilities for discussion, so little time!

---

## **Questions to Consider In-Depth**

***Add your question to Slido and vote on what questions we should try and address on Day Two -***

***<https://app.sli.do/event/tpinyvp7>***

**See Google Doc and/or GitHub agenda for link to W3C Community Slack.**

# Agenda - Day Two

- Recap of Day One and Intro to Day Two (10:00 - 10:10)
- Discussion
  - What Problem are We Trying to Solve? (10:10 - 10:40)
  - User Provisioning in a Mediated World (10:40 - 11:00)
  - AuthN vs AuthZ (11:00 - 11:15)
  - Browsers as Adtech Companies (11:15 – 11:20)
  - Legal Considerations (11:20 – 11:30)
- BREAK (11:30 - 11:45)
- Continuing the Conversation(s)
  - Documenting Scenarios (11:45 – 12:00)
  - When, Where, Who? (12:00 – 12:45)
- Wrap Up (12:45 – 12:55)



# What problem are we trying to solve?

- Is it conceivable that browsers mediating/owning the identity flows is not actually the desired objective? (13)
  - How many problems are already or better addressed through regulation, contracts or trust frameworks rather than deterministic technical enforcement in the UA? (2)
- The focus on privacy as the sole threat to be addressed seems to ignore other identity-related threats. How can we make sure to take other threats into account? (12)

# Problem Statement(s)

- Non-transparent, uncontrollable tracking of users across the web needs to be addressed and prevented.
- Federated login and tracking tools use the same primitives and are indistinguishable from non-transparent, uncontrollable tracking from the browser's perspective; browser's proposed mitigations for tracking will impact federated identity.

*This set of problem descriptions is still under discussion –  
consensus TBD.*

# User provisioning in a mediated world

- Sam: How would you imagine a user provisioning workflow in the IdP if the browser takes over the mediation? (10)
  - Id tokens as well as user info is usually signed by the IdP and checked by RPs. How will this be handled when the UA is the data holder and manipulates it? (8)
  - As email address is usually used to identify users, doesn't that need IdP support to set up multiple identities with different email addresses? (5)
  - re Kai's q about sigs: I think this is very important as feds are build around trust. The mediator breaks trust and now entities have to know about this mitm
  - Providing proxy emails is operationally expensive (Facebook did it 1st more than 10 years ago!) e.g. distributed spam reputation scores impact deliverability (1)

# Browsers as Adtech Companies

- 2/3 browsers today presenting are adtech and use tracking methods not included in the readme.  
Making the browser ID-mediator is conflict of interest? (7)

# AuthN vs AuthZ

- In the use case where the IdP communicates authorization attributes for an end user to access the SP, how do you see the authZ working when authN decoupled? (8)

# Legal considerations

- GDPR requires IdPs to ask for consent before data transfer to RPs. IdPs must log this consent. How will IdPs be able to do that when disconnected from the RPs? (13)
- From a regulatory perspective, is there a liability concern with browsers mediating identity flows where the "legal" relationship is between the IDP and the RP? (1)



# Continuing the Conversation

# Documenting Scenarios

- Vittorio Bertocci



# When, where, who?

- Does this group want to continue convening?
- Was this the right format?
- How often should it happen?
- Who else needs to be attending?
- Where else are discussions happening (which GitHub repositories, mailing lists, etc)? Can (should?) we consolidate these?