2023 INTERNET2 TECHNOLOGY exchange

BROWSER PRIVACY:
benefit or threat

REFEDS Browser Changes Working Group

Judith Bush, OCLC
Scott Cantor, The Ohio State University
Gary Windham, Cirrus Identity

Why are we here?

Federated identity is cross-site.

Browsers are mitigating cross-site tracking

- Third party cookies
- Navigational tracking
- And more.

Mitigations affect federated authentication.

Technical review, demo, then discuss possibilities.

Why do we care?

Third party cookies are a privacy threat and have little impact on SAML, OAuth, and OpenID Connect. Mitigations break logout, break discovery like Seamless.

Navigational tracking is also a privacy threat and mitigations threaten SAML, OAuth, and OpenID Connect.

FedCM solves third party cookies, doesn't depend on web primitives used in navigational tracking, but is incompatible with existing uses of SAML, OAuth, and OpenID Connect.

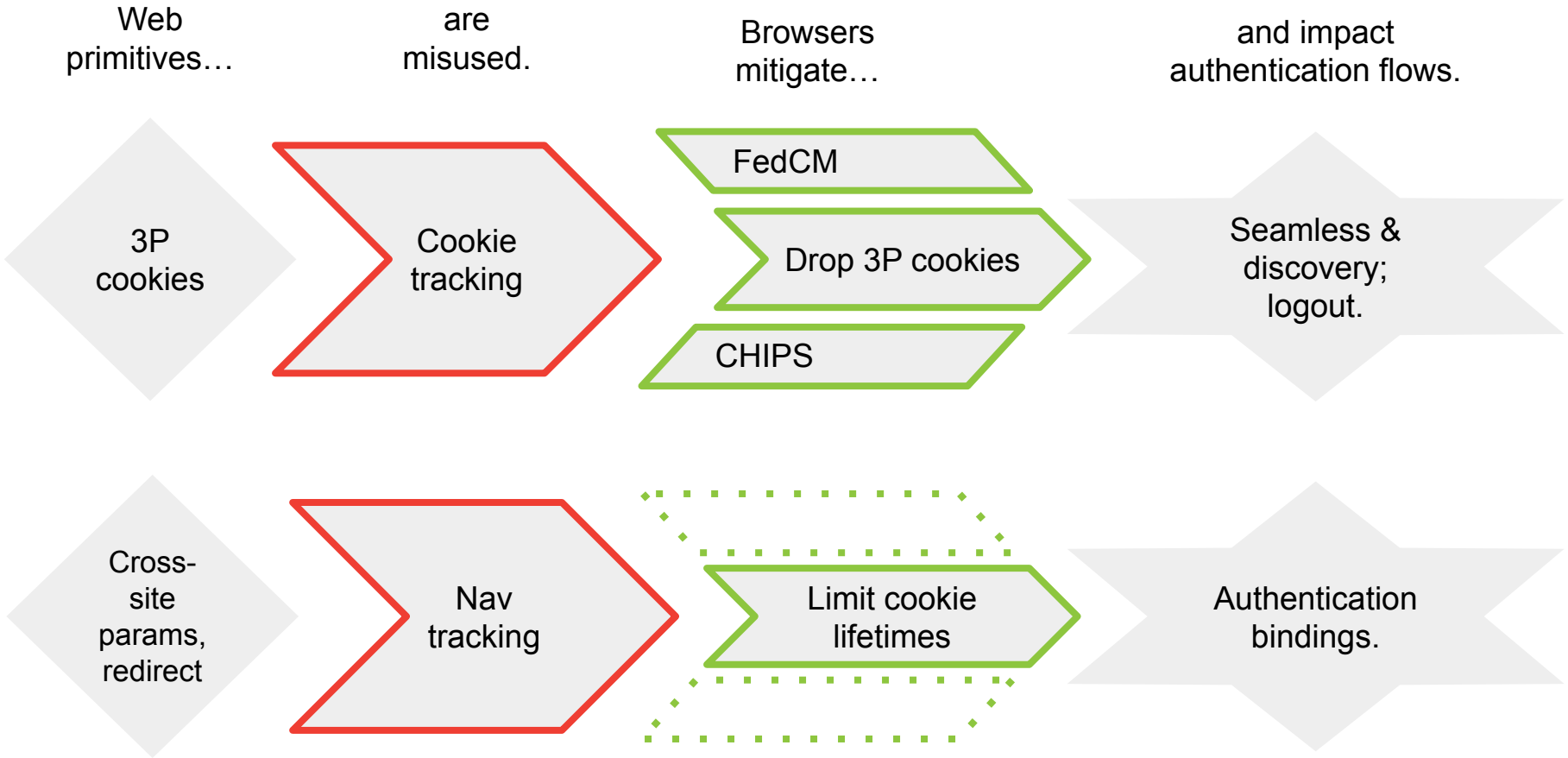
Technical Orientation

Threats and mitigations

Third party cookies

FedCM vs cookies

Navigational Tracking


Web primitives…
are misused.
Browsers mitigate…
and impact authentication flows.
3P cookies
Cookie tracking
FedCM
Drop 3P cookies
CHIPS
Seamless & discovery; logout.
Cross-site params, redirect
Nav tracking
Limit cookie lifetimes
Authentication bindings.

Understanding browser mitigation plans is ***important***:

it won't be ***urgent*** until too late.

We want you to understand how FedCM fits in the mitigation landscape:
it is an alternative to third party cookie uses in authentication, but not an alternative for authentication as we know it.

Mitigations to prevent navigational tracking are a threat to SAML and OIDC: FedCM may be offered as an alternative to cross-site redirects, link decoration.

We want you to help others - vendors, your institution - understand changes are occurring now, browser change roadmaps are short term compared to institutional time frames.

What is FedCM?

A way that a user can confirm to the browser that cross site information exchange can occur.

An authentication binding or profile that depends on the active intervention of the browser client.

A solution for authentication implementations that used **third party cookies** to ease the authentication user experience.

And also NOT COMPATIBLE with current usage of SAML or OpenID Connect.

What if FedCM is the only choice for cross site auth consent?

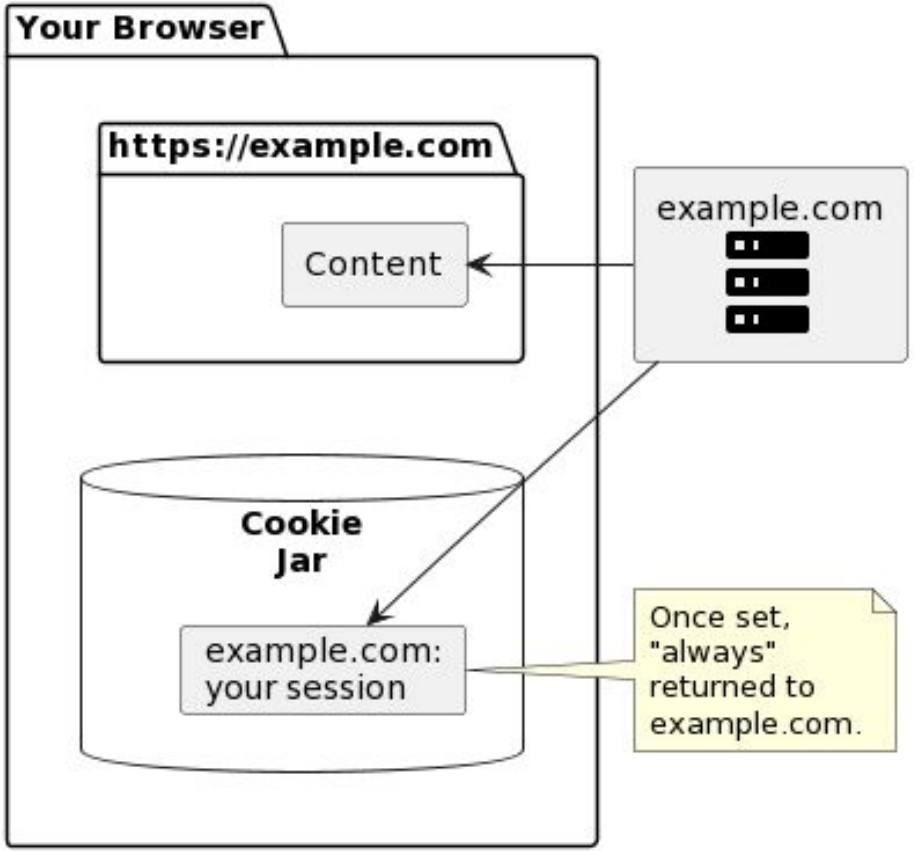
The OASIS SAML Technical Committee has been retired.

There is no obvious body to standardize SAML profiles to work within new navigational tracking mitigation constraints.

OpenID does not currently appear to have a profile for FedCM.

THIRD PARTY COOKIES

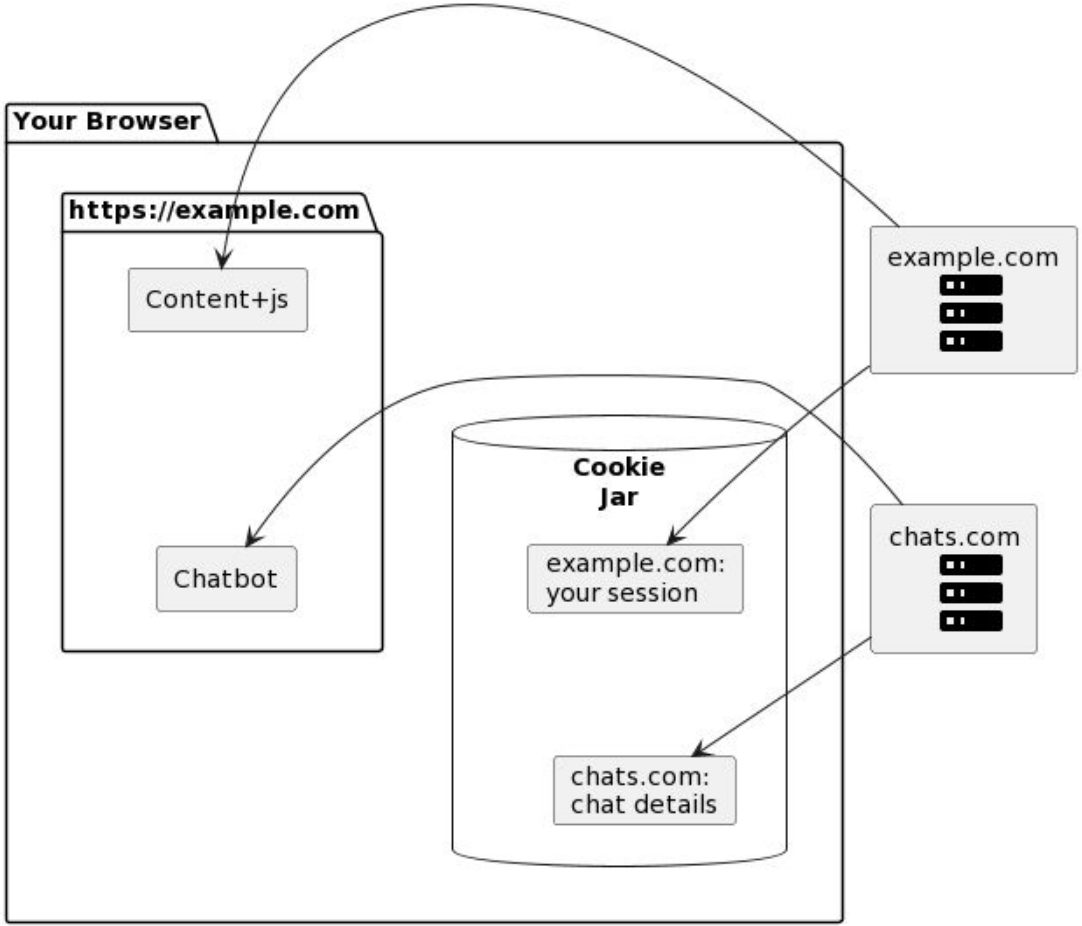
When the standards bodies refer to “sanctioned” tracking, they are referring to the interaction that is visible to the user.



THIRD PARTY COOKIES

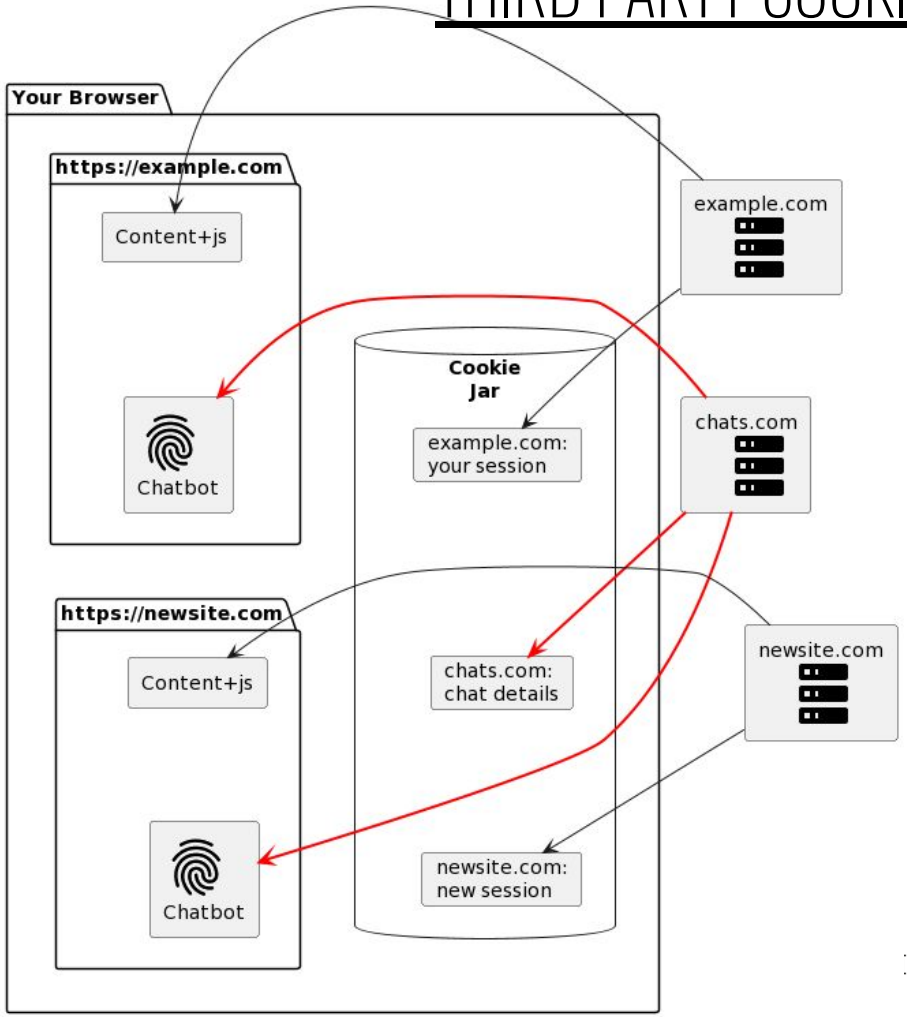
Third party relationships are not “visible” to the user, but make the web experience more rich.

Note the inclusion can be other types than javascript.



THIRD PARTY COOKIES

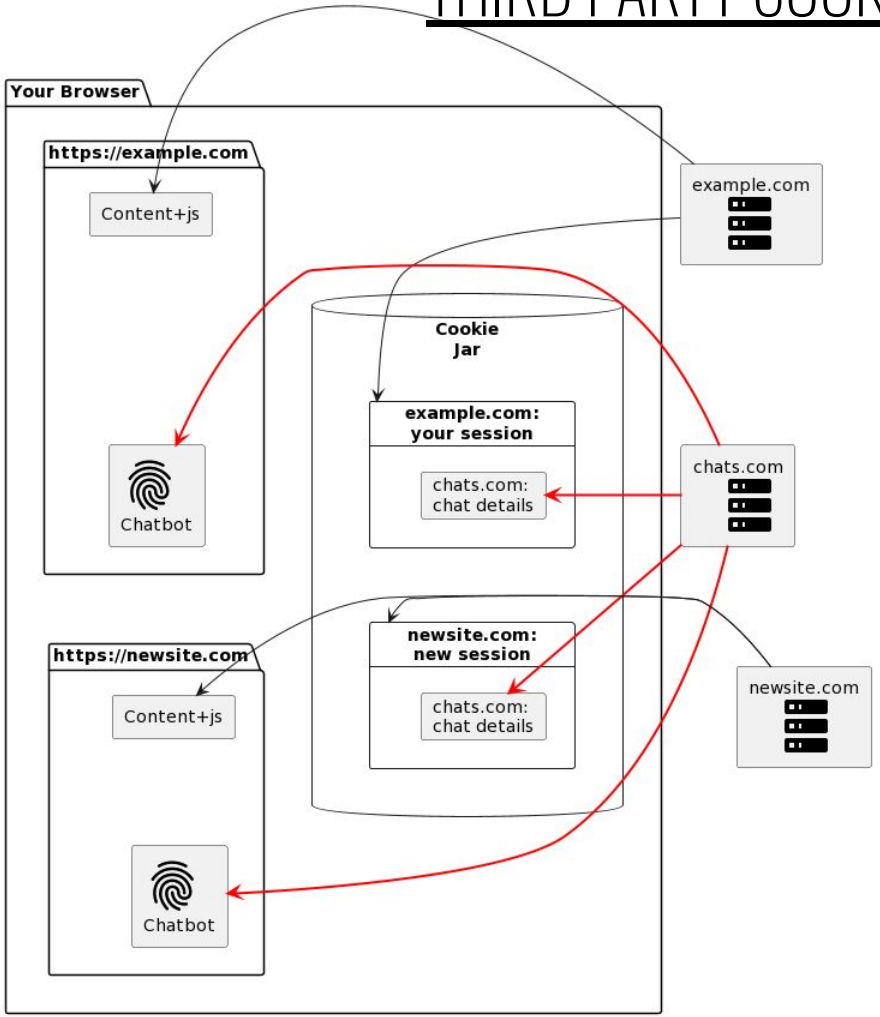
An unintended consequence: third party functionality “follows us around” the web, and led to an industry of trackers.



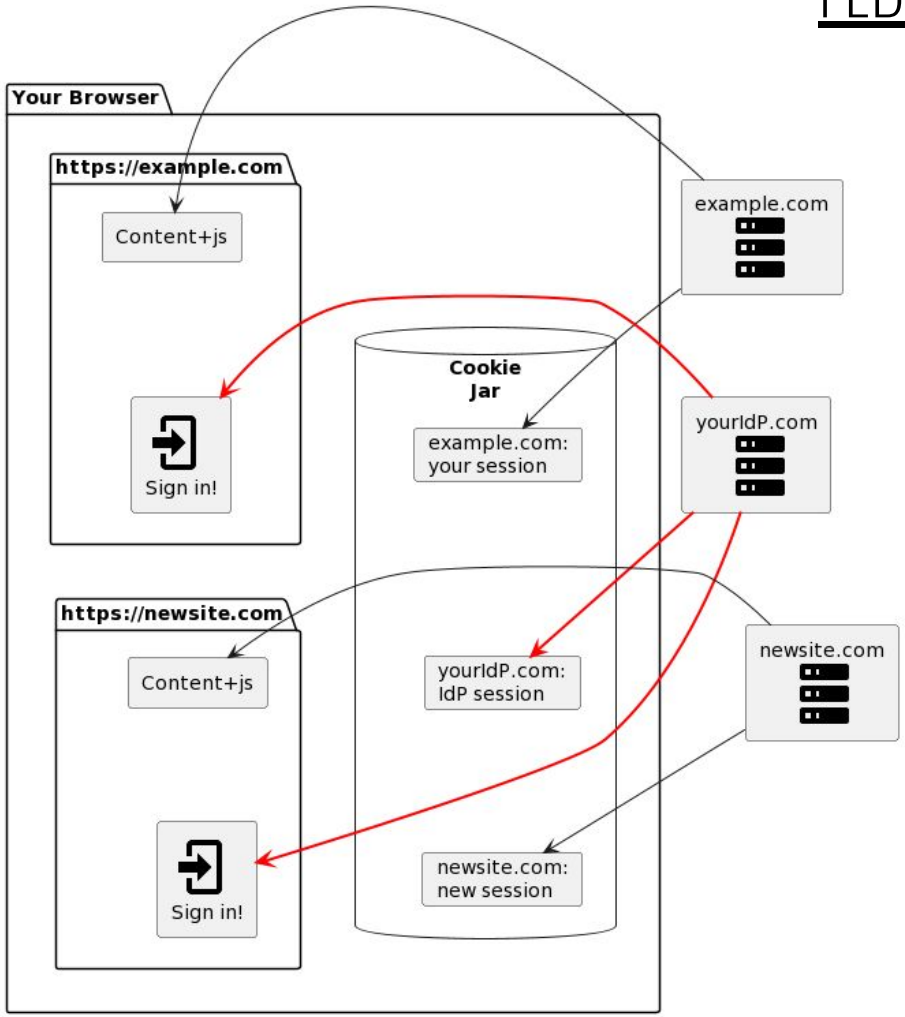
THIRD PARTY COOKIES

To keep third party functionality, but hamper the tracking, cookies are partitioned – **Cookies Having Independent Partitioned State (CHIPS)** – referrers are dropped, Chrome is considering proxy 3rd party calls, Safari and Firefox look for CNAME cloaking.

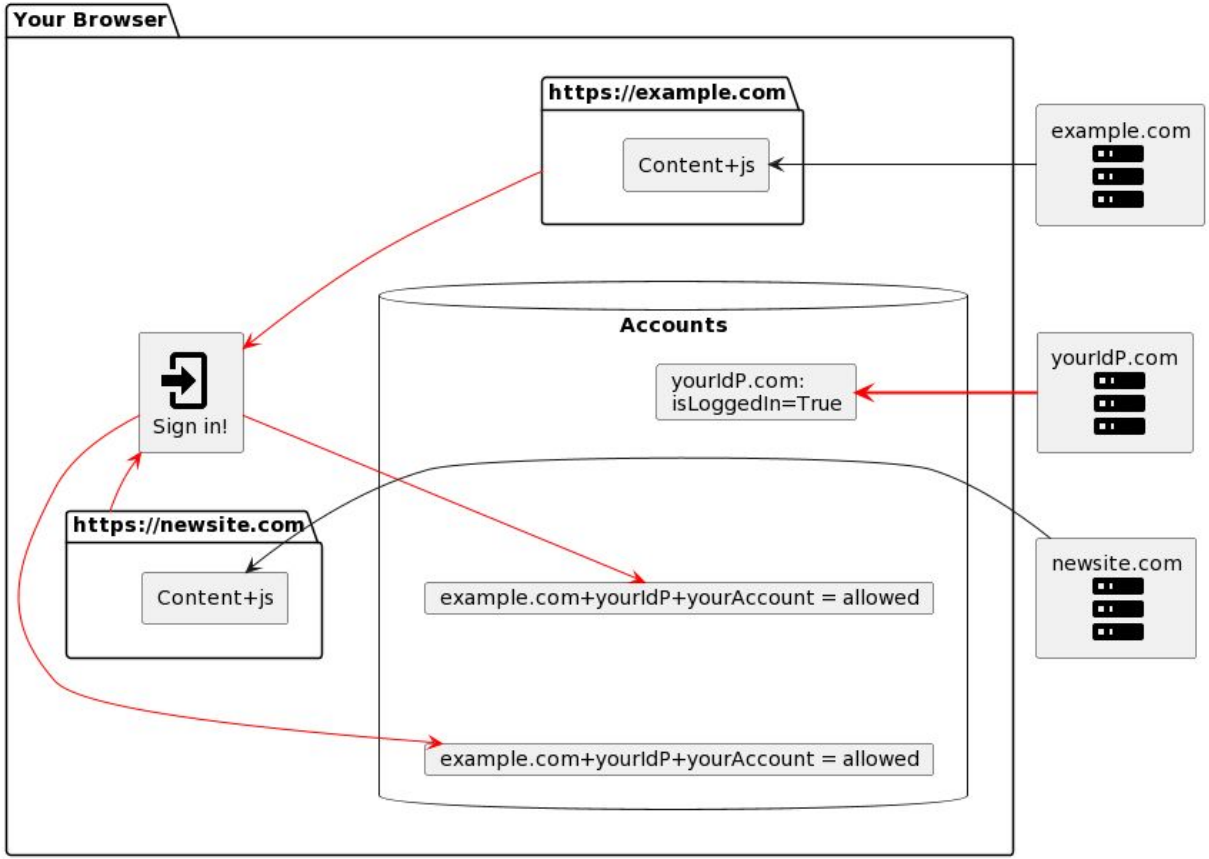
Other proposals are discussing ways to establish cross-site consent.



What if your IdP used an SDK that depended on 3rd party cookies? You need a solution outside of the cookie jar.



FedCM lets the IdP store state in the browser and allows the user, via the browser to mediate the connections.

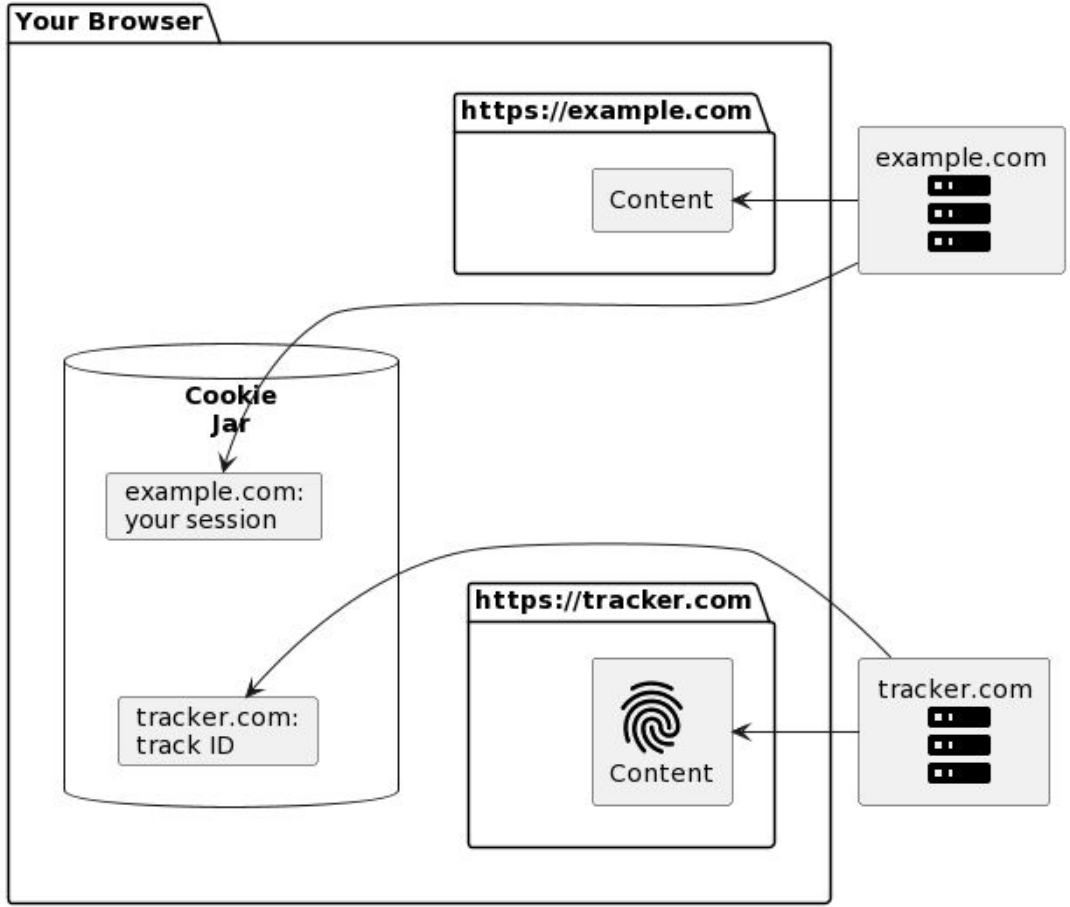


NAVIGATIONAL TRACKING

Why do we care?

SAML, OAuth, and OIDC don't depend on third party cookies.

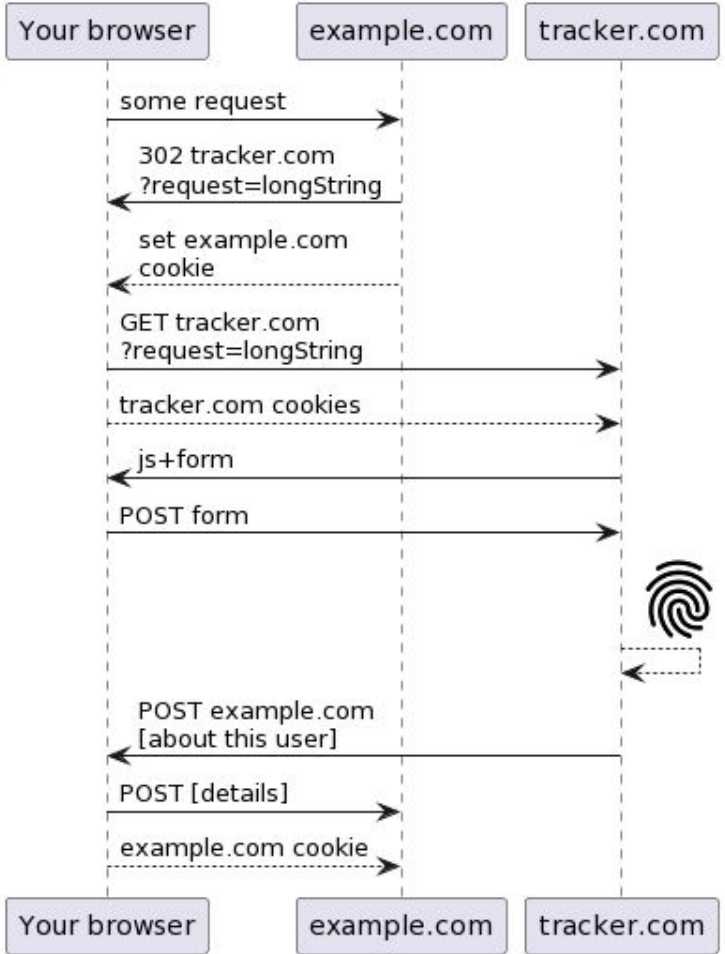
What cross-site communication is left?



NAVIGATIONAL TRACKING

There's a concept called "Navigational tracking" that includes "bounce tracking," using 302 redirects that redirect the user right back, and "link decoration", sending unique identifiers across sites.

How can this be distinguished from SSO?



FedCM and navigational tracking

FedCM is useful for IdPs that depended on integrations that used third party cookies.

Navigational tracking is a privacy concern and looks like SAML and OAuth flows.

Will navigational tracking mitigations eventually prevent cross-site redirects, link decoration, POST – because FedCM offers an alternative flow?

FedCM demo

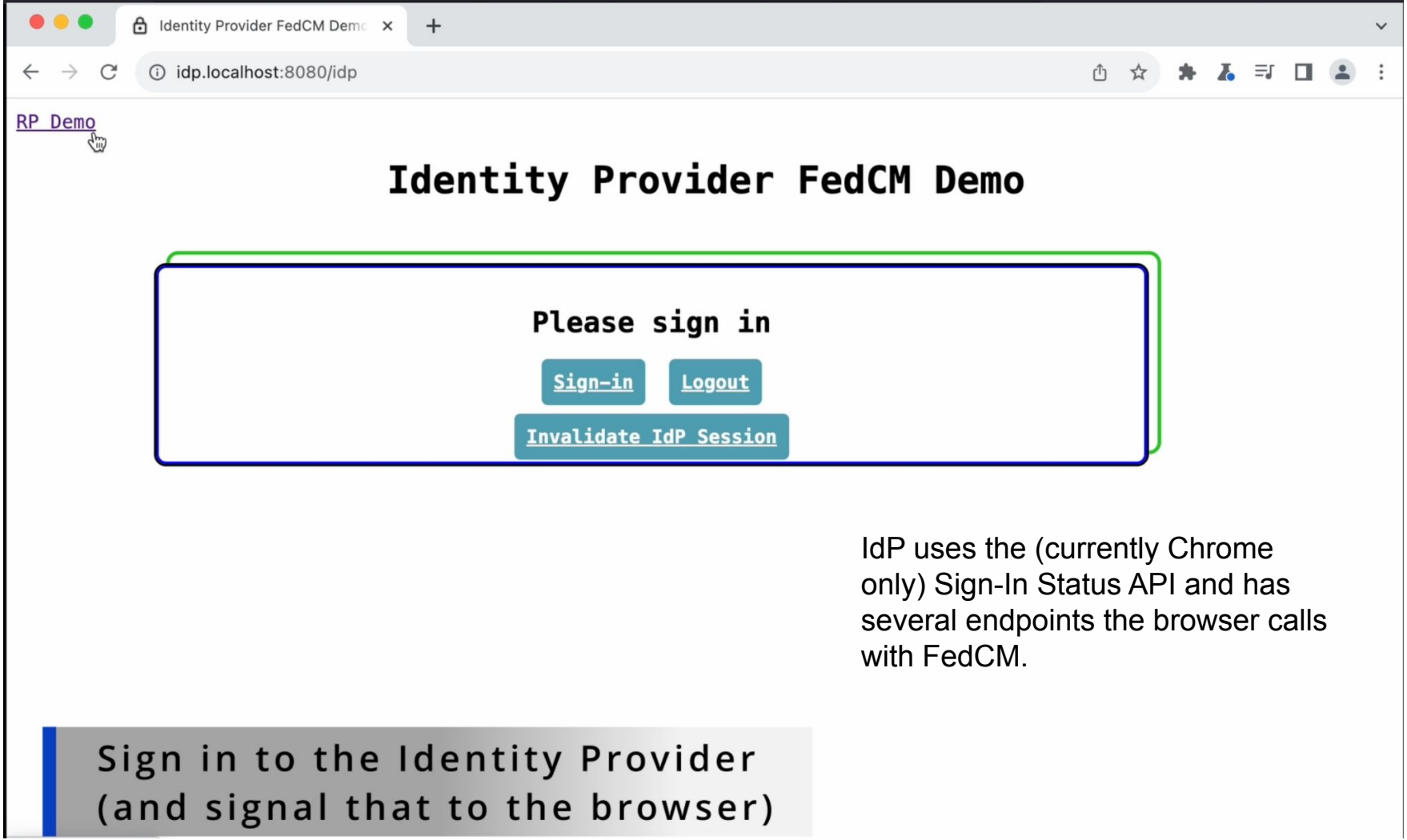
https://youtu.be/B3_f9BIA5cs?si=u20tclqMATusuOF7

Demo IdP and Sign-In Status API

Demo SP and FedCM

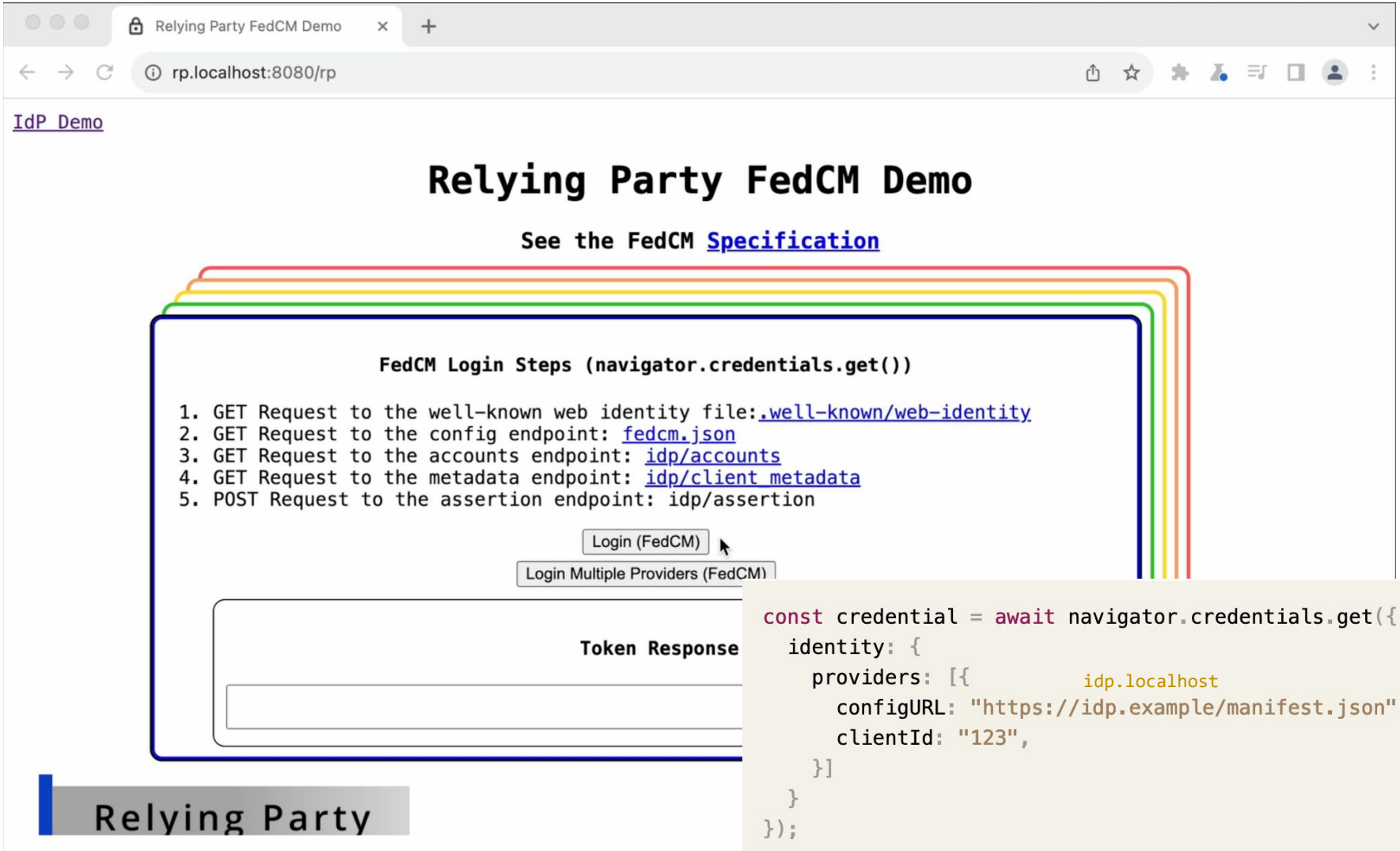
Video from Phil Smart: https://youtu.be/B3_f9BIA5cs?si=njWkZuxg-z-x16iC

Closer look at dialogue box

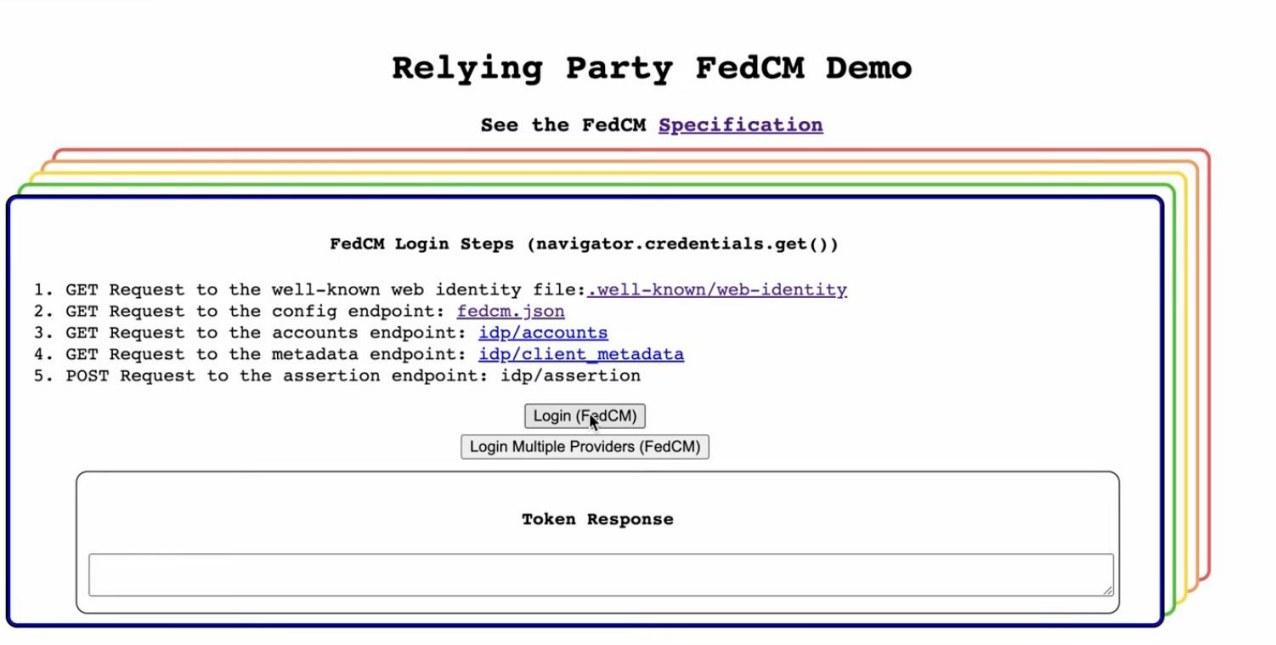


IdP uses the (currently Chrome only) Sign-In Status API and has several endpoints the browser calls with FedCM.

Sign in to the Identity Provider (and signal that to the browser)

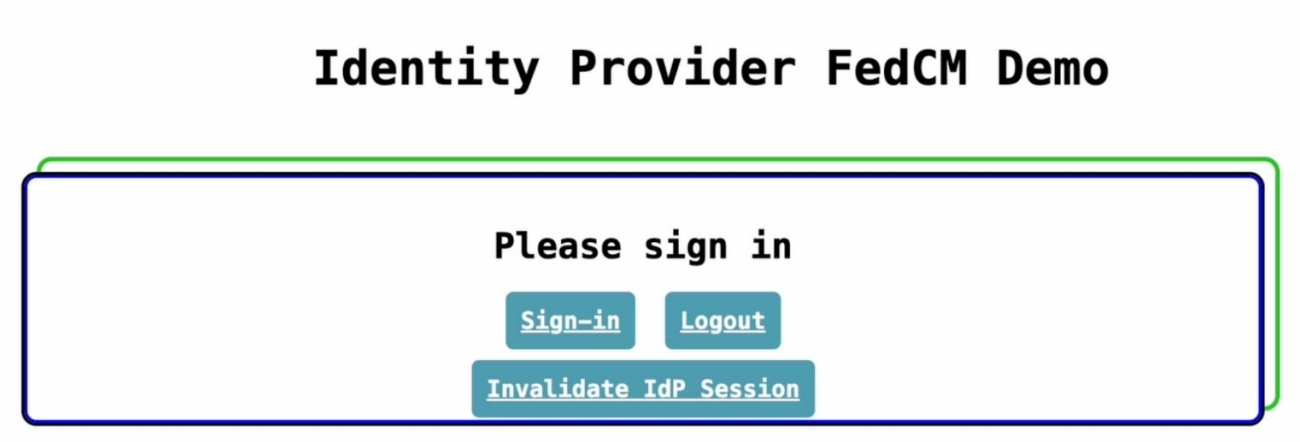

Relying Party FedCM Demo
rp.localhost:8080/rp
IdP Demo
Relying Party FedCM Demo
See the FedCM Specification
FedCM Login Steps (navigator.credentials.get())
1. GET Request to the well-known web identity file:.well-known/web-identity
2. GET Request to the config endpoint: fedcm.json
3. GET Request to the accounts endpoint: idp/accounts
4. GET Request to the metadata endpoint: idp/client_metadata
5. POST Request to the assertion endpoint: idp/assertion
Login (FedCM)
Login Multiple Providers (FedCM)
Token Response
const credential = await navigator.credentials.get({
identity: {
providers: [{
idp.localhost
configURL: "https://idp.example/manifest.json",
clientId: "123",
}]
}
});
Relying Party

VIDEO ALTERNATIVE



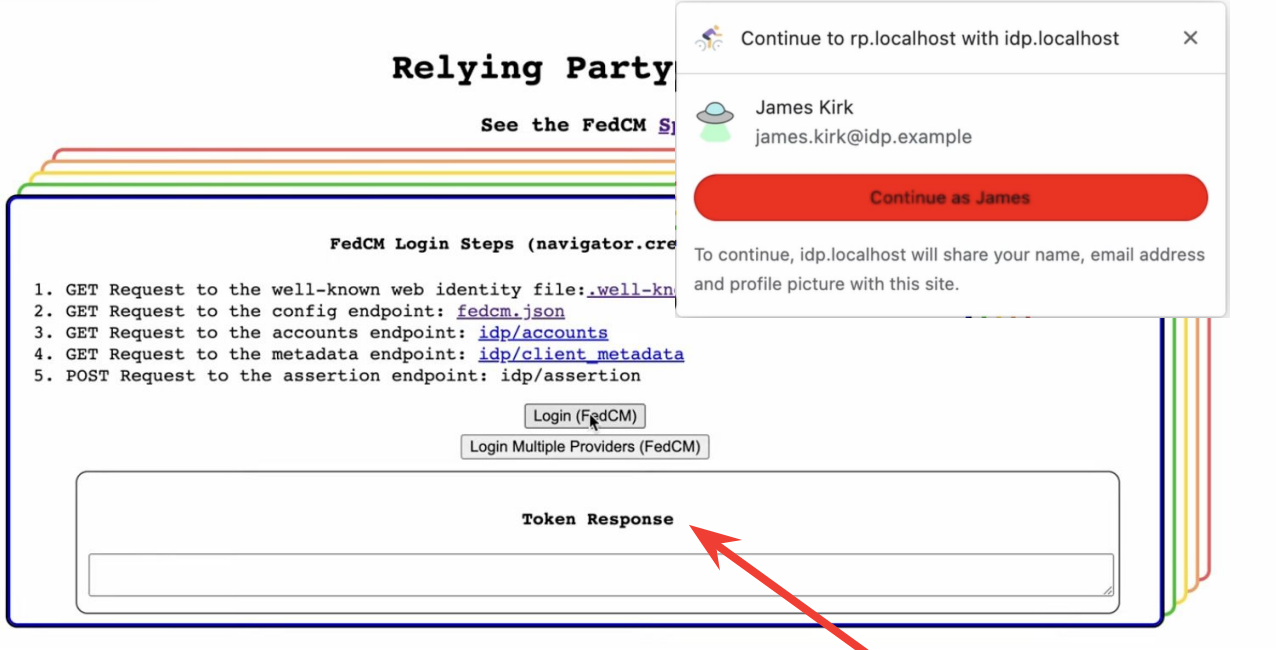
User arrives at a FedCM relying party/service provider, fails to authenticate because IdP has not set browser state.

VIDEO ALTERNATIVE



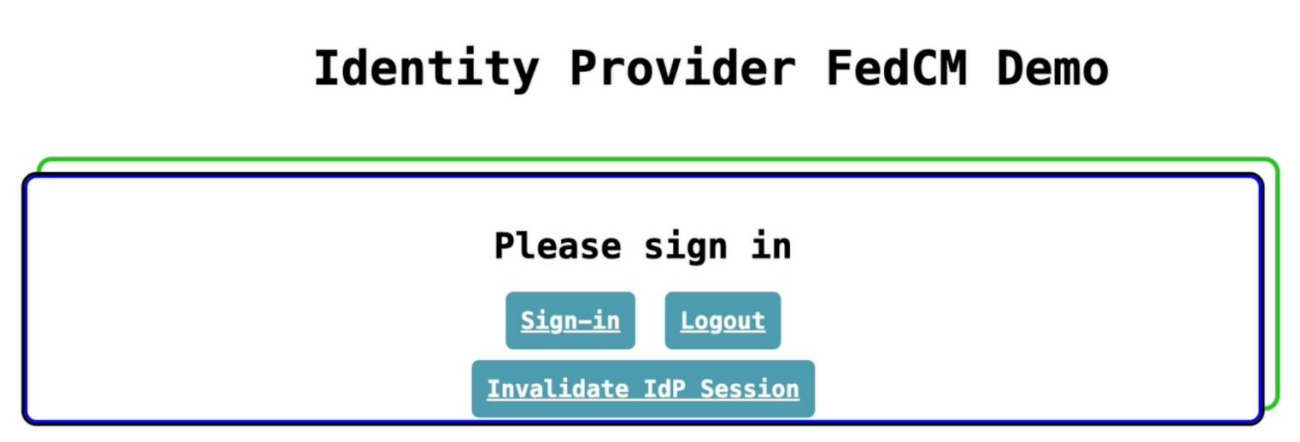
User signs on at identity provider, which also sets browser state.

VIDEO ALTERNATIVE



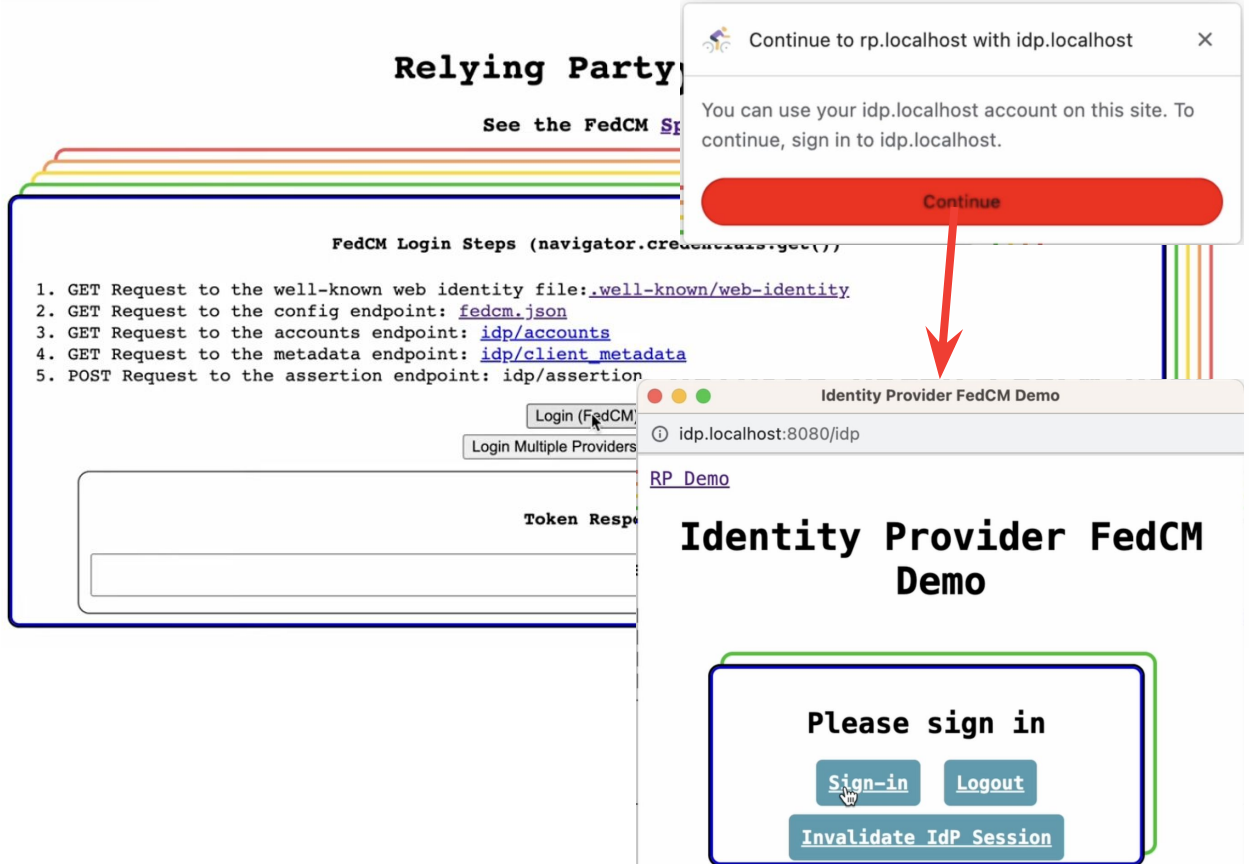
Now when user attempts at RP, the browser is able to create a dialogue. On consent, the browser relays a “token” – some string – from the IdP to the RP.

VIDEO ALTERNATIVE



Consider the case where the browser state is unchanged, but the session at the IdP is no longer active.

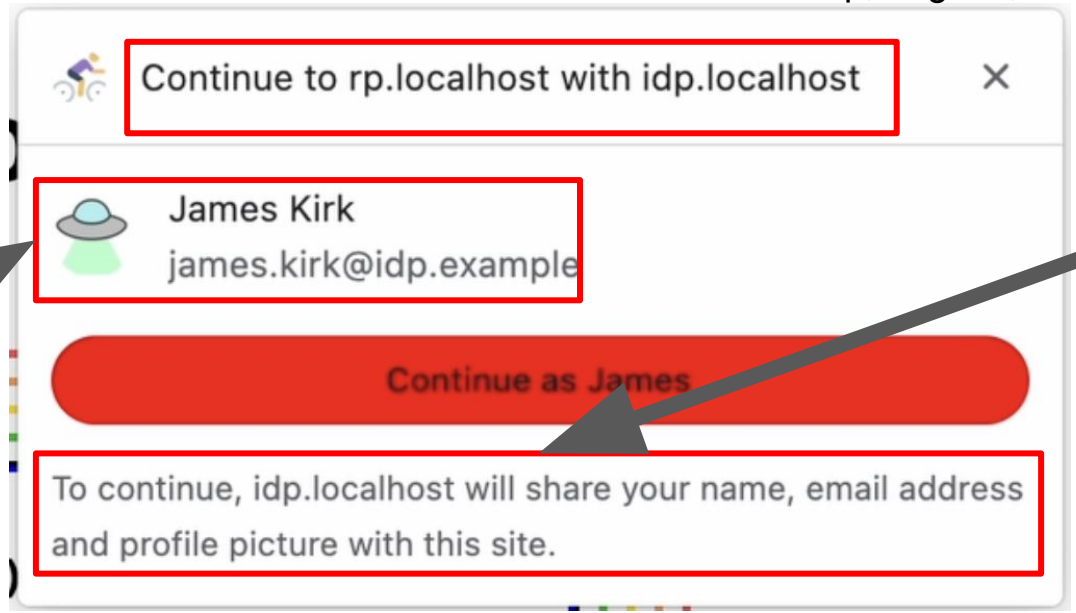
VIDEO ALTERNATIVE



Now when user attempts at RP, the browser is unable to receive any accounts from the IdP. If the user continues, browser pops open a window to the IdP with the current capabilities of the main browser. Success at the IdP then creates the original flow.

A closer look at the FedCM dialogue

The language, look, and feel is under the control of the browser. Some verb alternatives can be specified: ‘sign up,’ ‘sign in,’ and ‘use.’



Supports disambiguation between multiple accounts at same IdP

Standard OIDC data elements (claims). May change as authZ is discussed.

FedCM and established authentication protocols

April 2023 “solution”

More problems, other possibilities

April 2023 “solution”

Before the Signin status API

Discovery outside FedCM and no third party cookies: user trusts RP with selections

Consent at every hop challenging to explain to user

RPs could identify by entity ID

No (explicit) support for communicating assurance, ForceAuthn requirements

User does not have any assurance regarding IdP data shown by browser

More problems, other possibilities

Signin status API would require initial engagement with every hop. Proxies are not being considered.

Possible that first party engagement must be maintained (every ~45 days).

… log out …

A future where user consent required for all cross-site interactions with “local storage” model.

Understanding browser mitigation plans is ***important***:

it won’t be ***urgent*** until too late.

FedCM not fit for our rich ecosystem

Mitigations to prevent navigational tracking are being discussed, but not currently at the level of third party cookie issues.

Changes are occurring now.

W3C WG discussions need member participation representing our community so that assumptions such as “I don't think there will be specific protocol implementation issues” do not go unchallenged.

Discussion

Assuming severe navigational tracking mitigations, what might be the best outcomes for our community?

What alternatives to cross-site browser consent flows might be in the future? What if SPs adopt FedCM?

Your questions?

ACAMP topics?

Resources

Summary of current state of different types of browser mitigations:
https://wiki.refeds.org/display/GROUPS/State+of+browser+privacy+evolution
Other slides, blogs, and videos:
https://wiki.refeds.org/display/GROUPS/Slides%2C+blogs%2C+and+videos

FedCM Specification https://fedidcg.github.io/FedCM/

W3C Working Group Proposed Charter
https://github.com/fedidcg/fedidcg.github.io/blob/main/charters/Proposed-WG-WebIdentityCredentials.md