Federated Identity & The Federated Credentials Management API

Kristen Chapman
kristen.chapman@salesforce.com

What Is Identity Federation?

OAuth, OpenID, SAML, Federated Identity Management, authorization vs. authentication, credentials, SSO, security domains, and so on and so and so on...

There are a lot of terms associated with identity federation - and it's often pretty confusing.

At its most basic, though, identity federation is simply about linking an individual's digital identity across different sites or services.

(example: using a Twitter account to log in to a media site)

Why Talk About It Here?

1

Advertising

is arguably one of the economic backbones of the web

2

Federated Identity

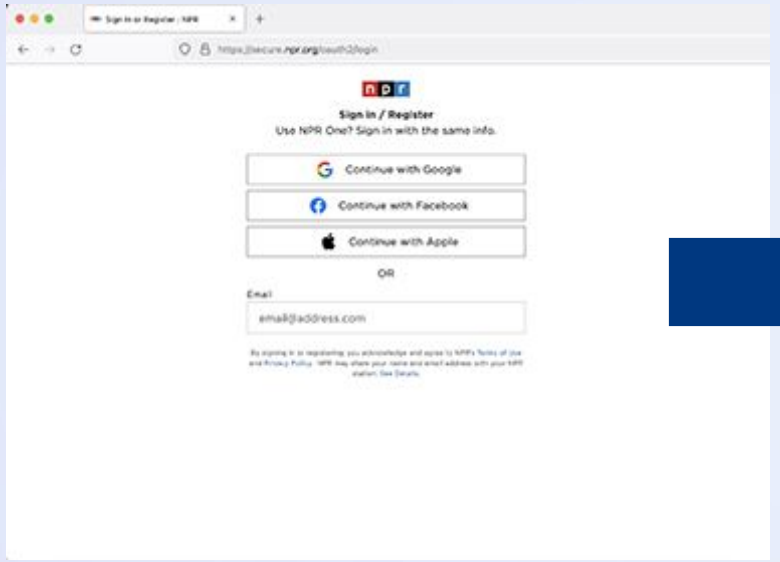
could be considered one of the usability backbones of the internet

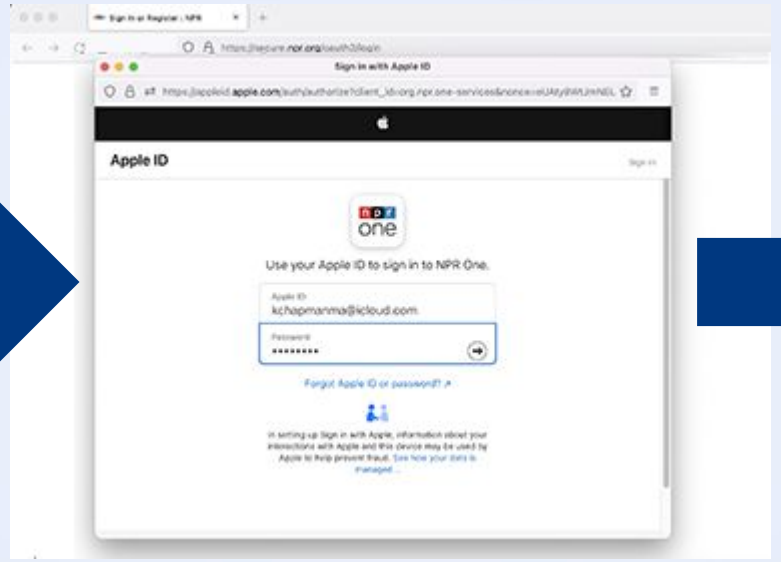
3

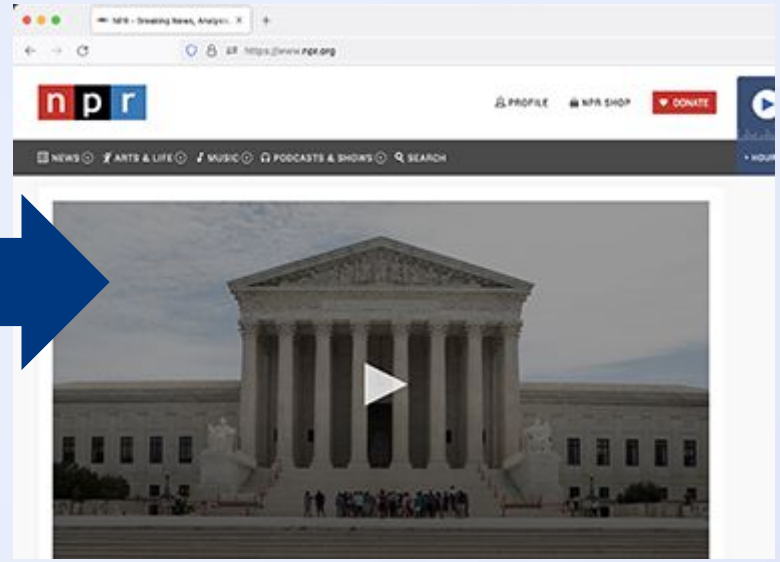
The Overlap

is they both rely on the same web primitives: third-party cookies, link decoration, etc .

One Example Of Federated Identity







Clicks to login to a site

User can choose to login directly to the site or with an Identity Provider

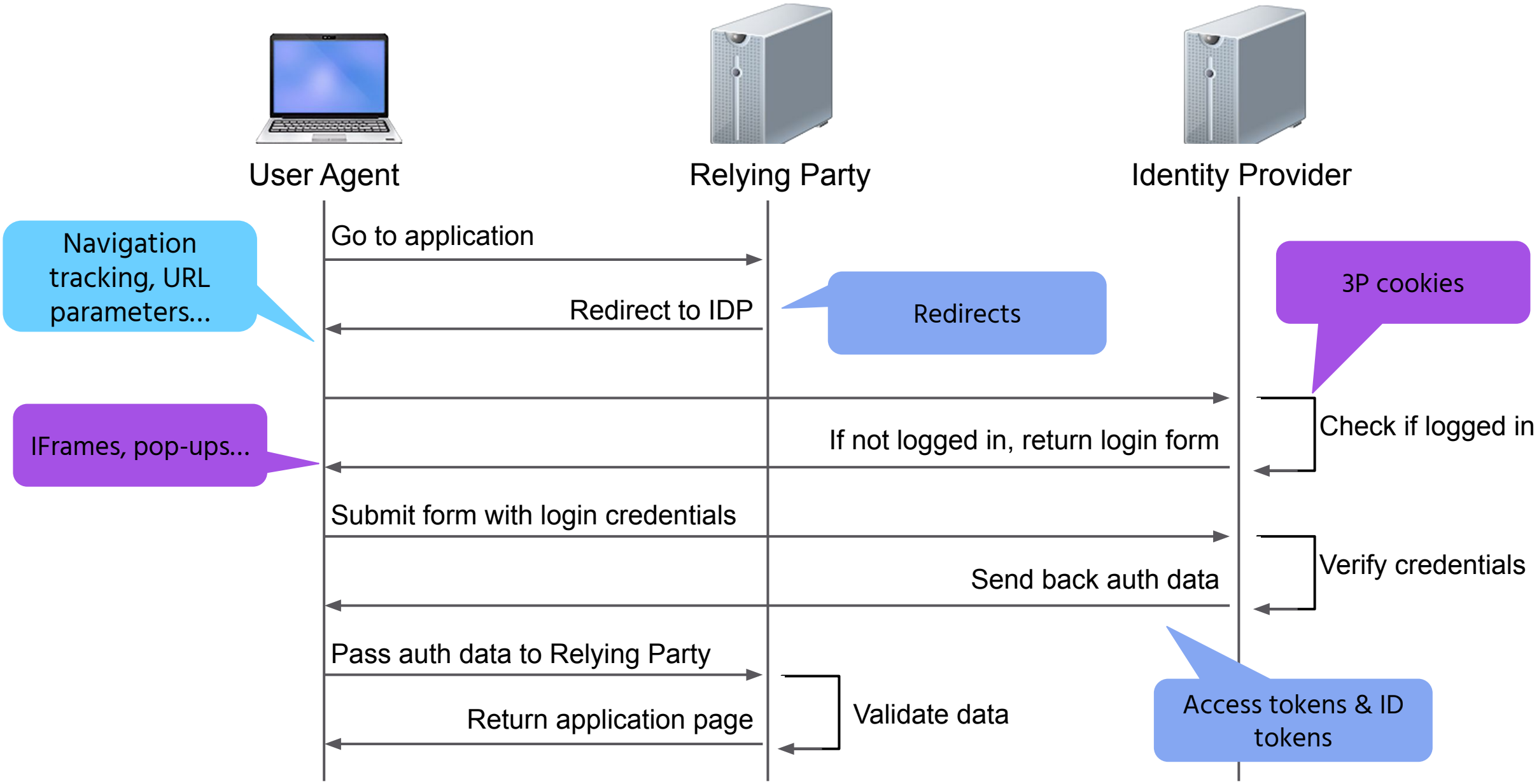
Chooses an Identity Provider

If they're not logged in, presented with the login form for the IDP

Back to the Relying Party

With the Identity Provider sending back authentication / authorization data

Behind The Scenes



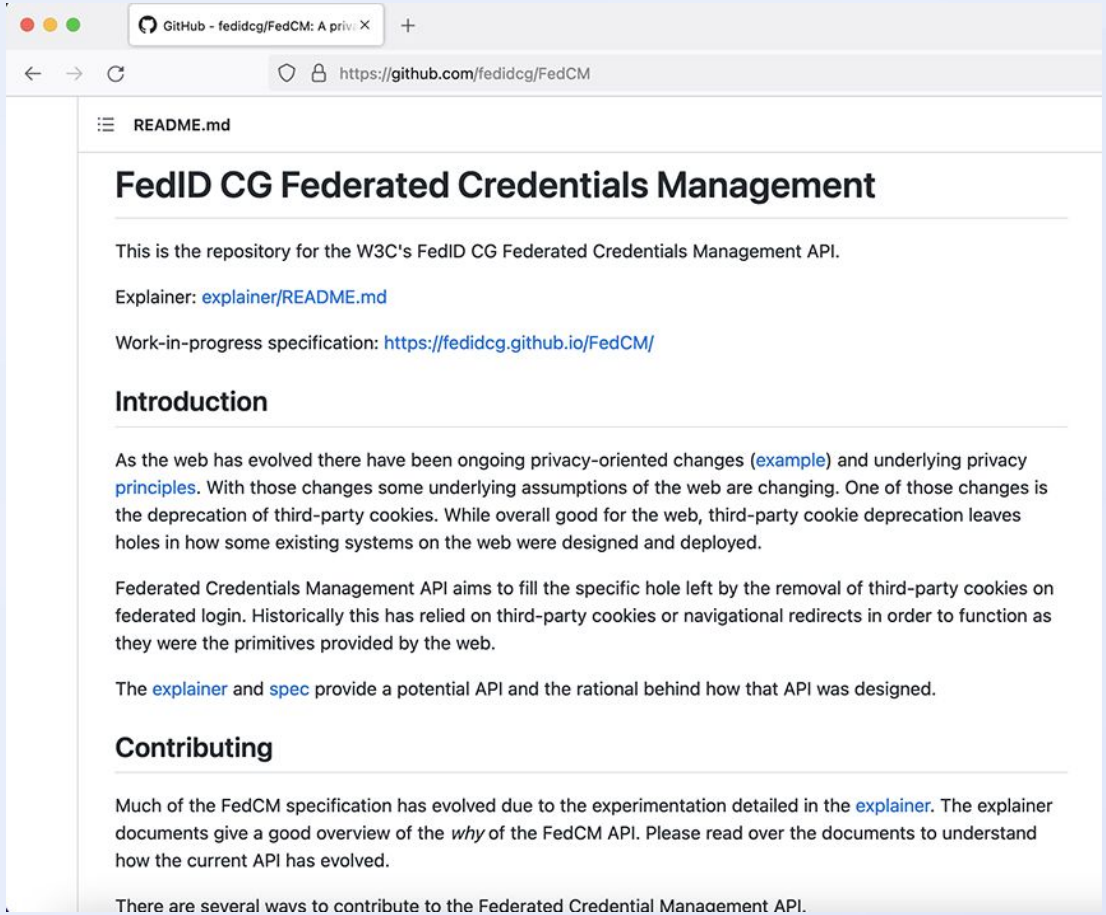
Some Of The Challenges Involved

- Many of the proposed privacy changes for tracking will also disrupt federated identity.
- It has its own privacy concerns since it can also be used to collect data about users:
  - Identity Providers can see which sites a user visits
  - Relying Parties can learn information about the user from the Identity Provider
  - Often uses global identifiers like email addresses
- It's a massive problem. Identity federation has been around a long time - and different protocols (SAML, OAuth, OIDC, etc.), implementations and use cases have evolved online.
- It's used by very diverse institutions: B2B, B2C, B2E, financial, federal, health services, universities for both students and researchers, etc.
- The solution can't require all of these different parties to do too much work, or it won't be feasible in a timely manner.

Federated Credentials Management API

Formerly Known As WebID

- This is Google's proposal for how to support Federated Identity without third-party cookies.
- It's currently only focused on the third-party cookie dependency, since that's the most pressing change.
- They are also trying to require the least amount of work from Relying Parties (the Sites/Services).
- It's actively being discussed in the Federated Identity CG.



Google Considered Three Alternatives

Permission-Oriented

The user-agent tries to warn users about potential tracking risks - and prompts the user for their permission to continue.

Mediation-Oriented

The user-agent acts as a mediator between the Relying Party and the Identity Provider. The user-agent can then control what data is exchanged.

Delegation-Oriented

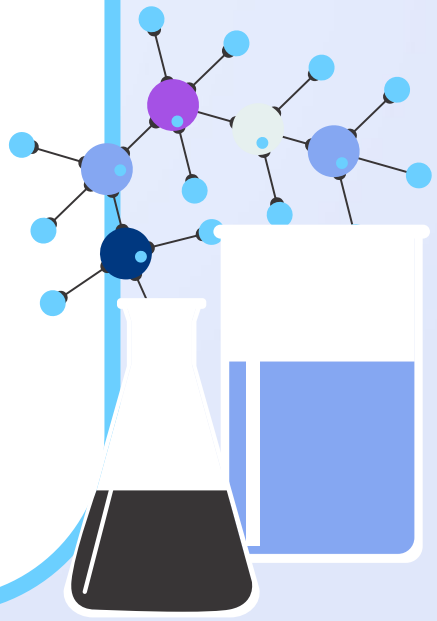
The user-agent still acts as the mediator - but in this scenario they take over more work from the Identity Provider to stop the IdP from observing which sites the user is visiting.

Mediation-Oriented Is The Focus For Now

Graphic by Google

The Use Cases Google Considered

- Sign-Up
- Sign-In
  - Prompted Sign-In
  - Auto Sign-In
- Sign-out
  - Relying Party
  - Identity Provider
- Session Management
- Revocation / Account Cancellation
  - With the Relying Party
  - With the Identity Provider
- Authorization
  - The user also has access to the resources

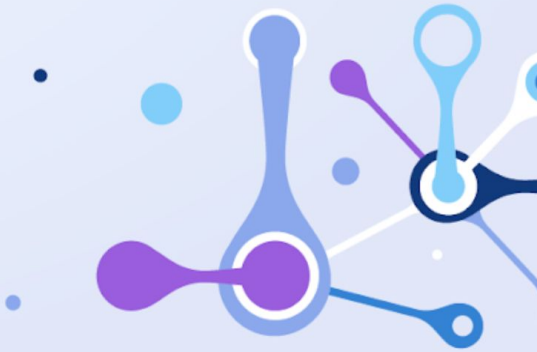


The Current Status

- The FedID CG is gathering and documenting different use cases, and working with Google on the proposal.
- Outstanding questions/concerns:
  - What should the role of the user-agent be here? Many of the browser vendors are also identity providers, which is problematic.
  - Google and Microsoft are active in the FedID CG - but we really need more involvement from the other browsers. Will they support the FedCM proposal or are expecting other APIs to be used?
  - What's the relationship going to be like between the privacy APIs in general in terms of federated identity?

For More Information

- Identity vs. Browser Changes video from the 2021 OAuth Security Workshop: PDF of the slides
- Authentication vs. Federation vs. SSO overview article
- Common Federated Identity Protocols: OpenID Connect vs. OAuth vs. SAML 2.0 on HackEDU
- Federated Identity articles on ScienceDirect
- FedCM Proposal: https://github.com/fedidcg/FedCM
- The FedCM HOWTO
- FedCM Draft Report: https://fedidcg.github.io/FedCM/
- FedCM at BlinkOn 15: video and slides
- FedCM at TPAC 2021: video and minutes



Thank You!

If you'd like to join the FedID CG, you can do so at:
https://www.w3.org/community/fed-id/

Another Example Of Federated Identity

Employee