Issue #374

CHAPI over FedCM

An Early Exploration

goto@google.com

Jan 2023

What's FedCM?
Where do we expect it to go?
What are some shared interests?
What are some tensions?

What’s FedCM?

Why?

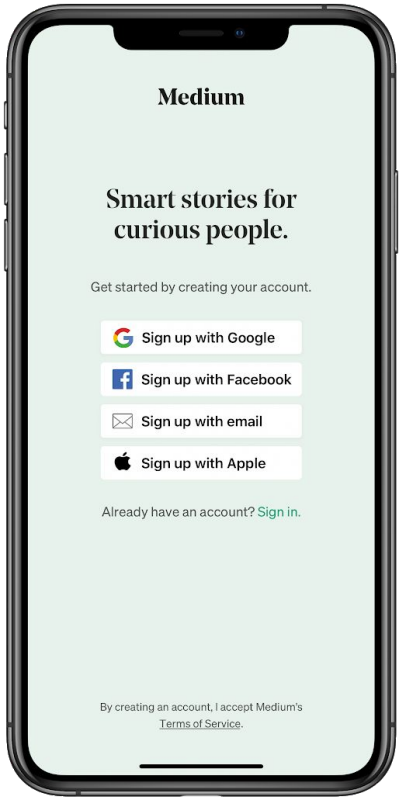
Federated Identity

What is it?

Users sign-in to a RP (relying party) with an IdP (Identity provider)

Why do we think it's important?

Federated identity is safer* than per-site usernames and passwords



* phishing, password reuse, etc

Why?

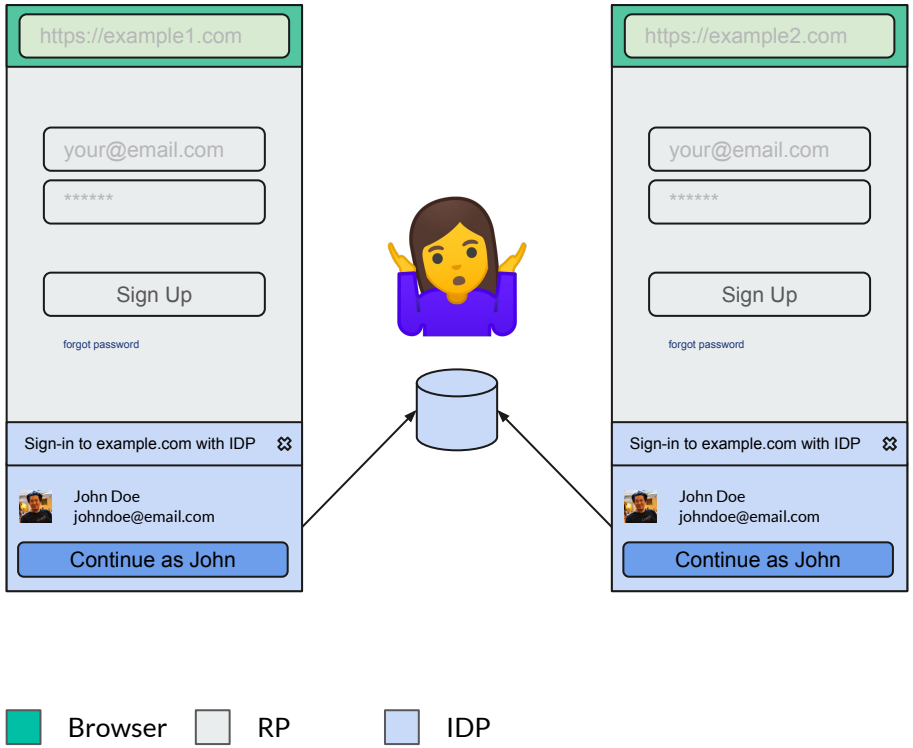
What's the problem?

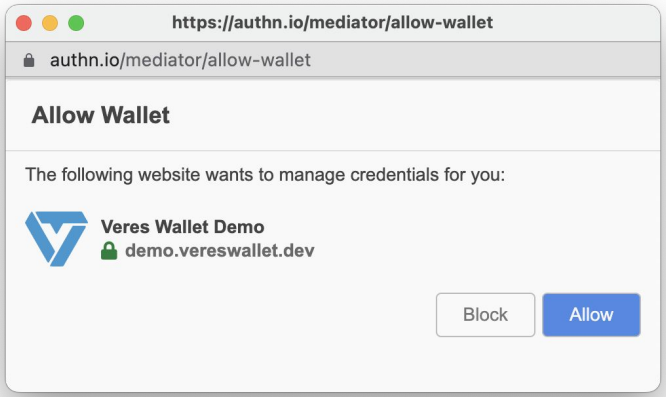
By design, identity federation was built on top of low-level primitives*.

By accident, the same primitives also enable cross-site tracking.

* iframes, third party cookies, redirects

The Classification Problem





For example, in the absence of third party cookies, CHAPI degrades* gracefully** to popups.

* by degradation, I mean that it exposes, for example, the user to https://authn.io.

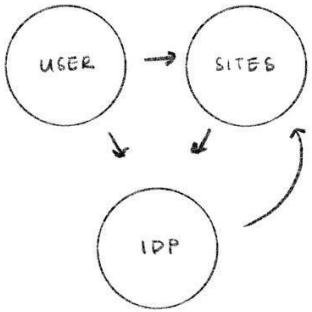
** by graceful, I mean that it still able to operate.

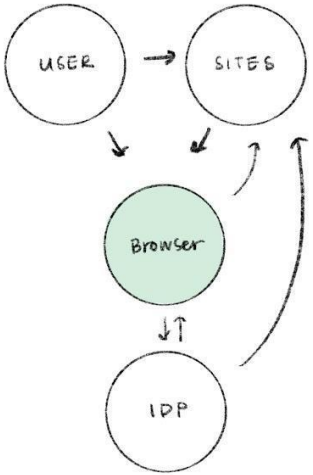
What's FedCM*?

A high-level *, identity-specific, privacy-preserving browser API that enables identity federation to continue to thrive on the web.

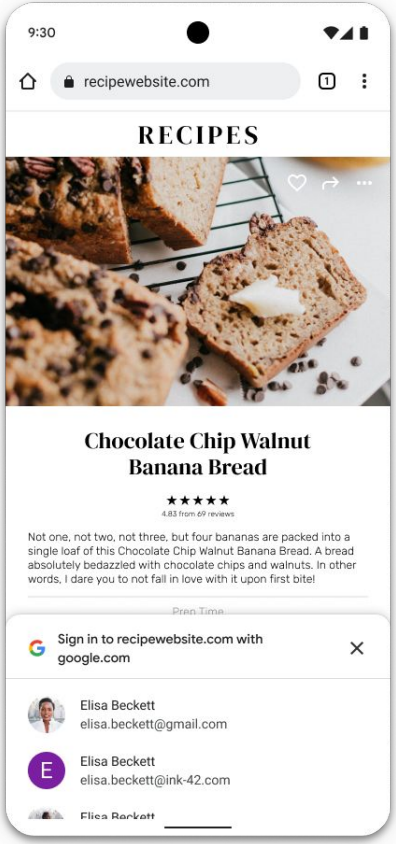
Preservation followed by Extension.

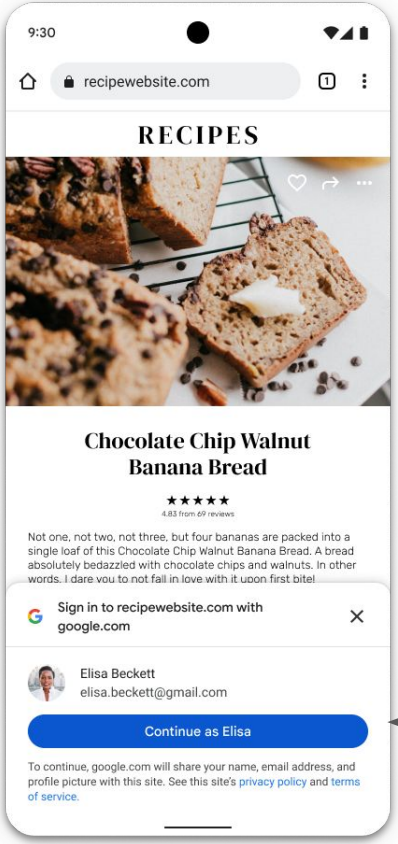
* high-level vs low-level APIs make a trade-off between, among other things, expressivity and control.





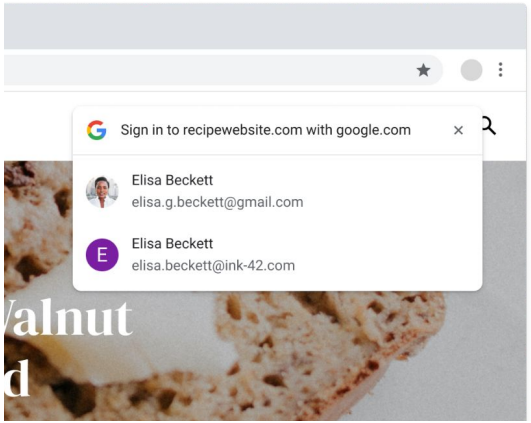
What is FedCM?

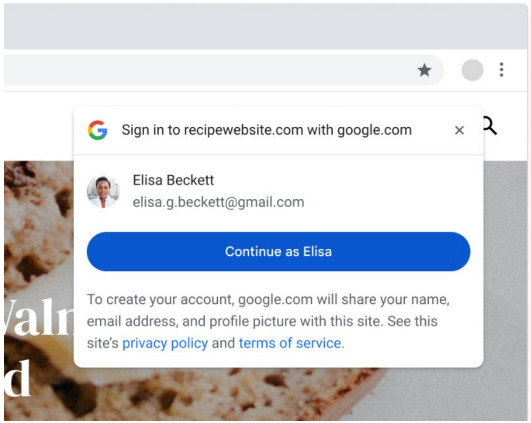


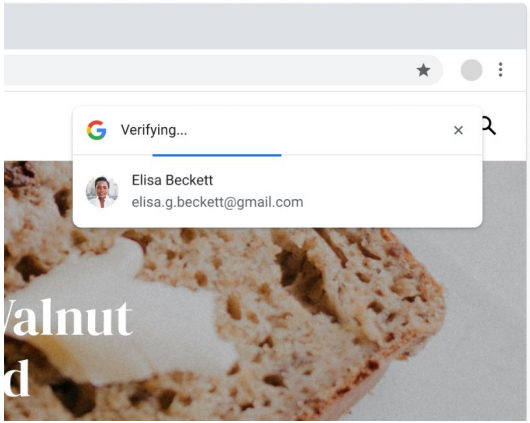


Works without third party cookies!

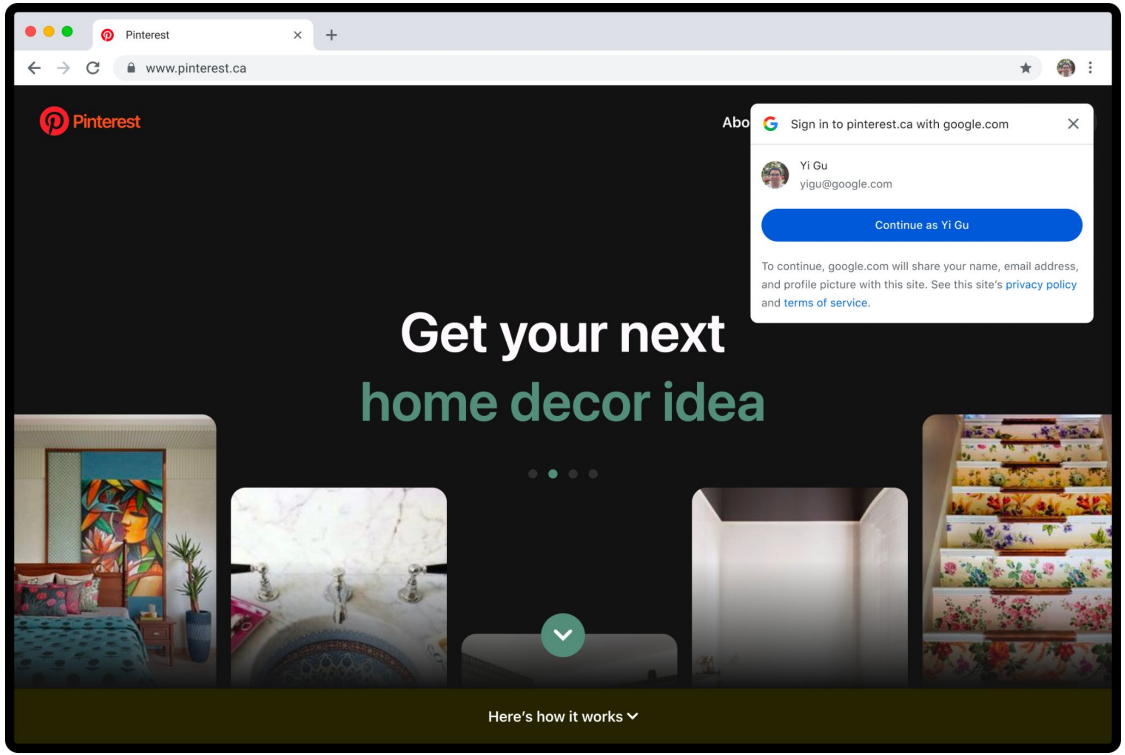
What is FedCM?





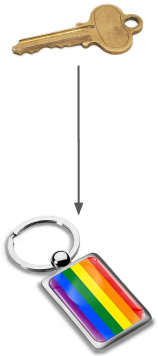


Available publicly in chrome since M108

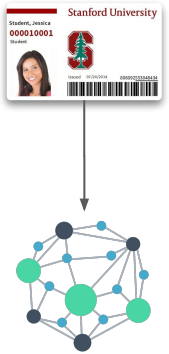


Where is it going?

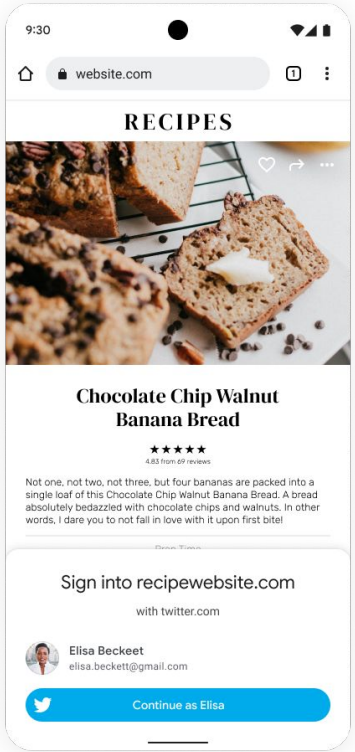
Web **Authentication** manages my keys.

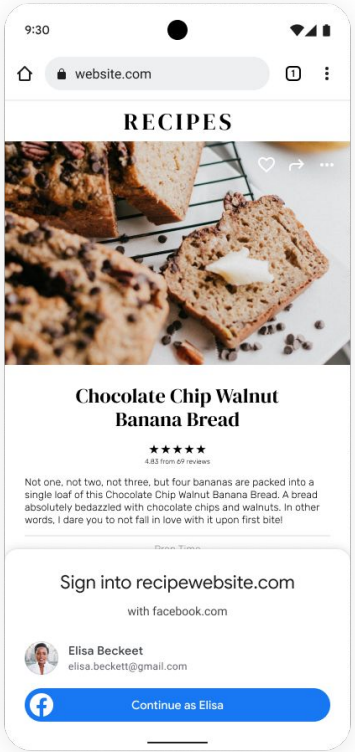


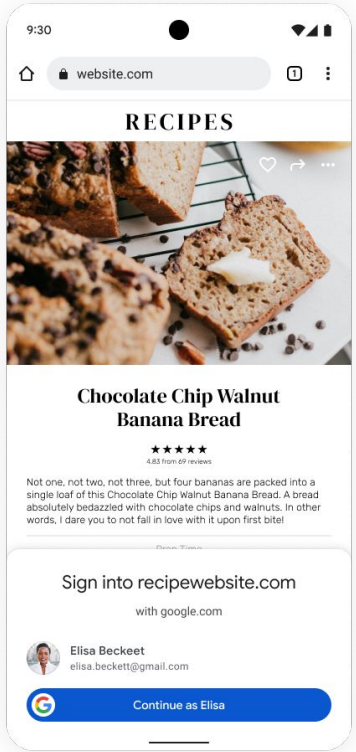
Web **Identity** manages my identity.

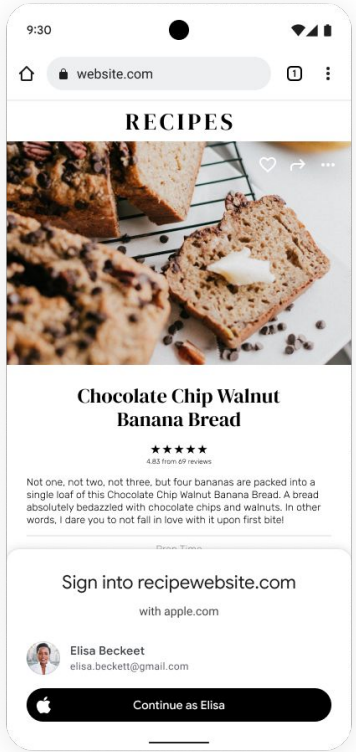


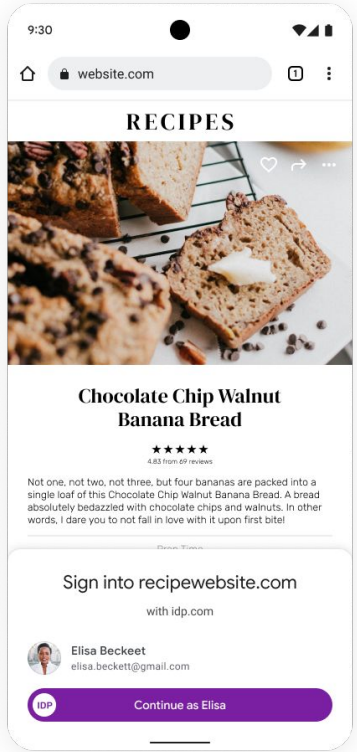
We expect WebAuthn to play an increasingly important role in, as its name suggests, authentication.





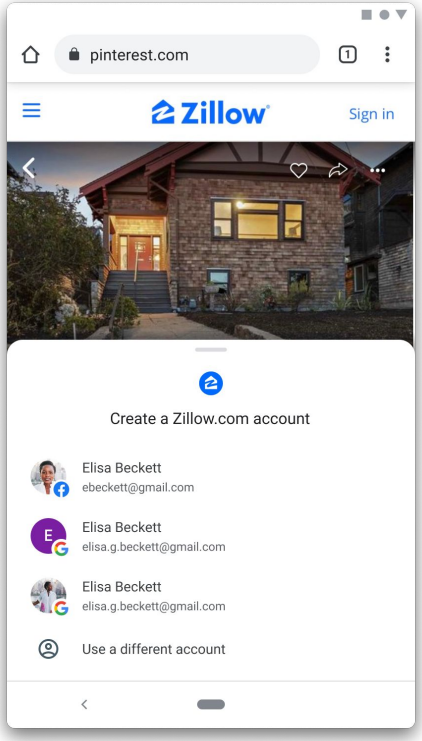






You should be able to represent yourself in many ways.

Early Mocks

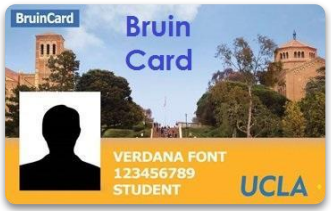


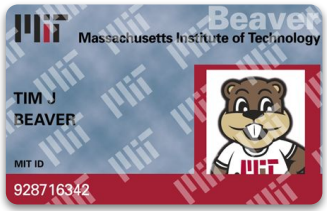
You should have a choice of how you present yourself online.

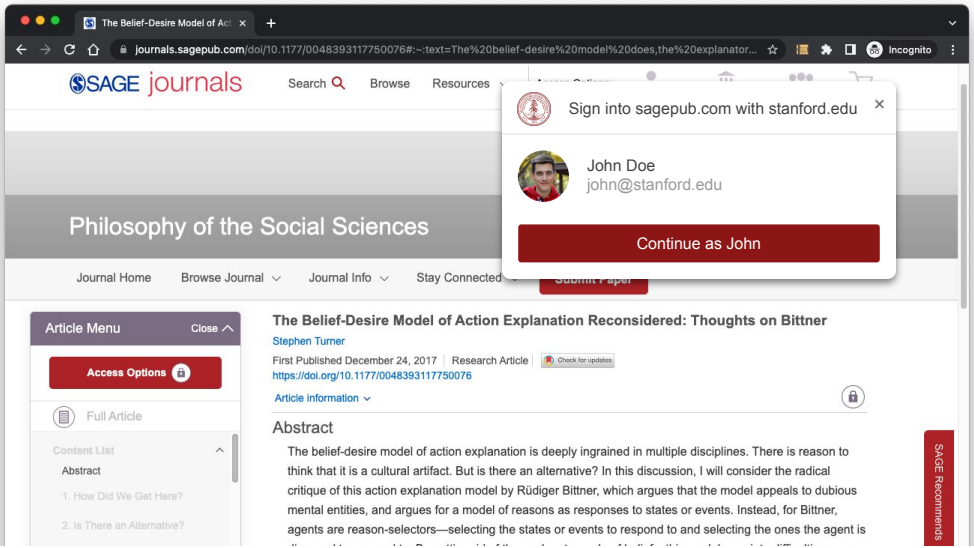
Student IDs

[Issue #29]

Illustrative Mock
NOT ready to build







You should be able to bring your Student ID to do your online research.

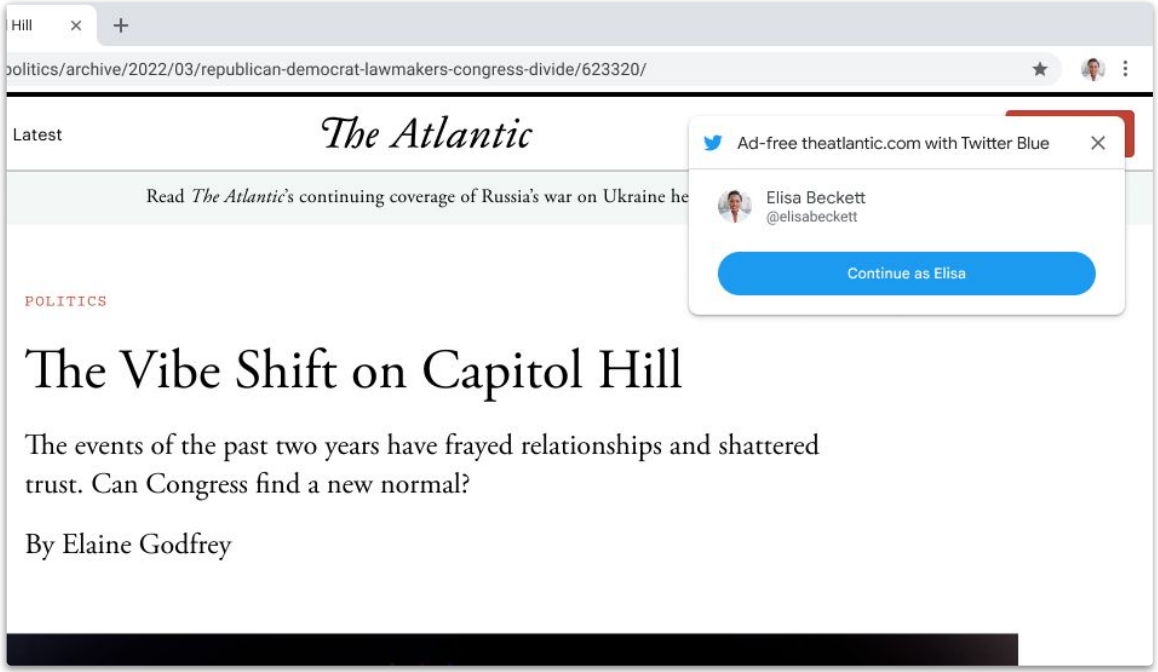
My Membership IDs

Early Mocks

LATERPAY

Premium

Subscribe with Google

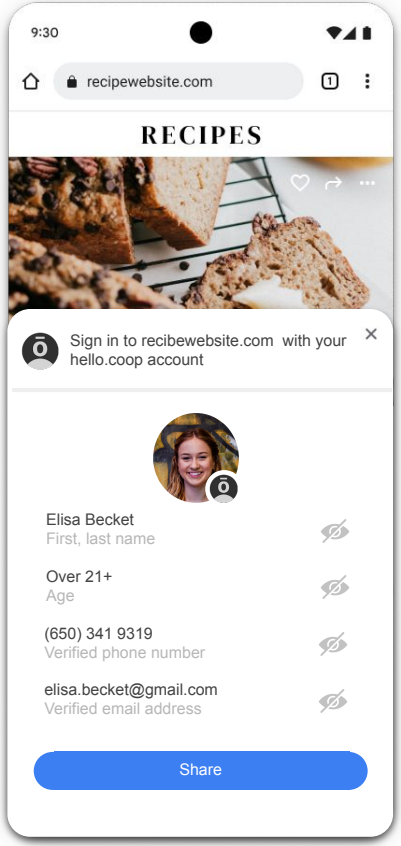


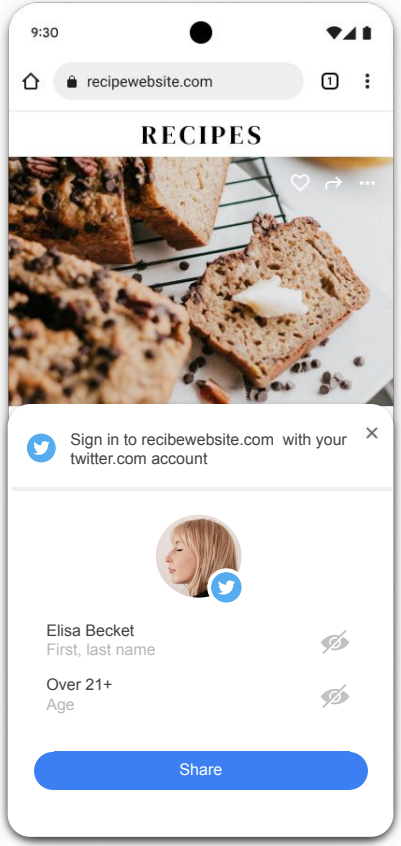
You are a member of a variety of discount clubs. You should be able to bring your membership cards everywhere you go.

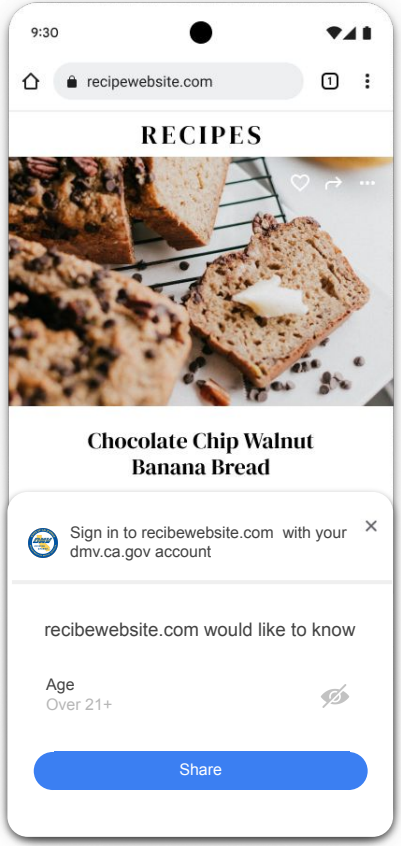
Illustrative Mock
NOT ready to build

Selective Disclosure

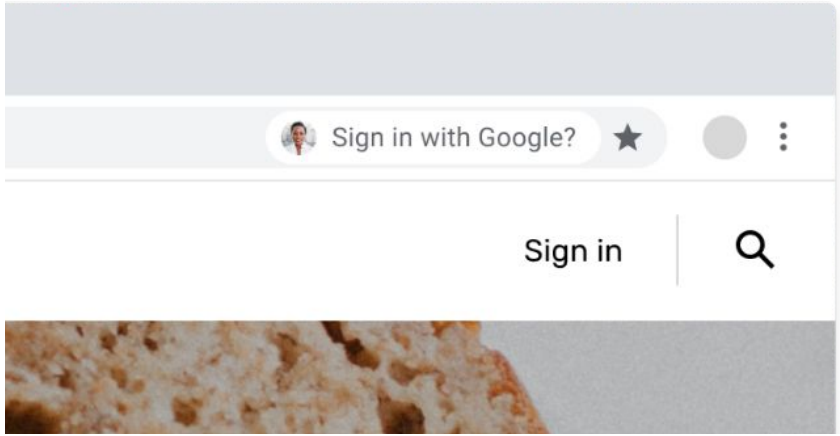
Issue #242







Early Mocks



Your site identity should be a first class citizen in Browser UX.

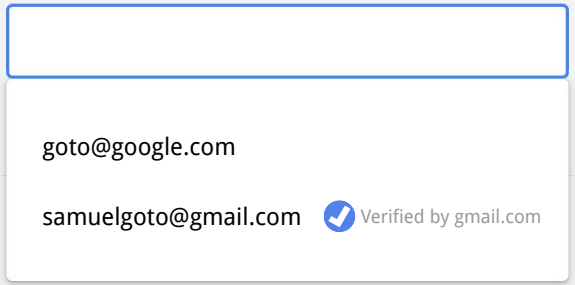
Early Mocks

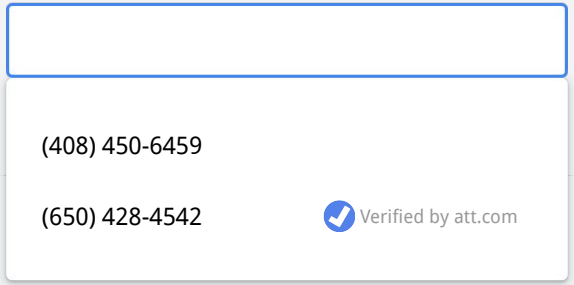
Verified Autocomplete

Websites annotate their forms accepting providers:

```
<form providers="https://accounts.google.com">
  <input type="email">
  <input type="tel">
</form>
```

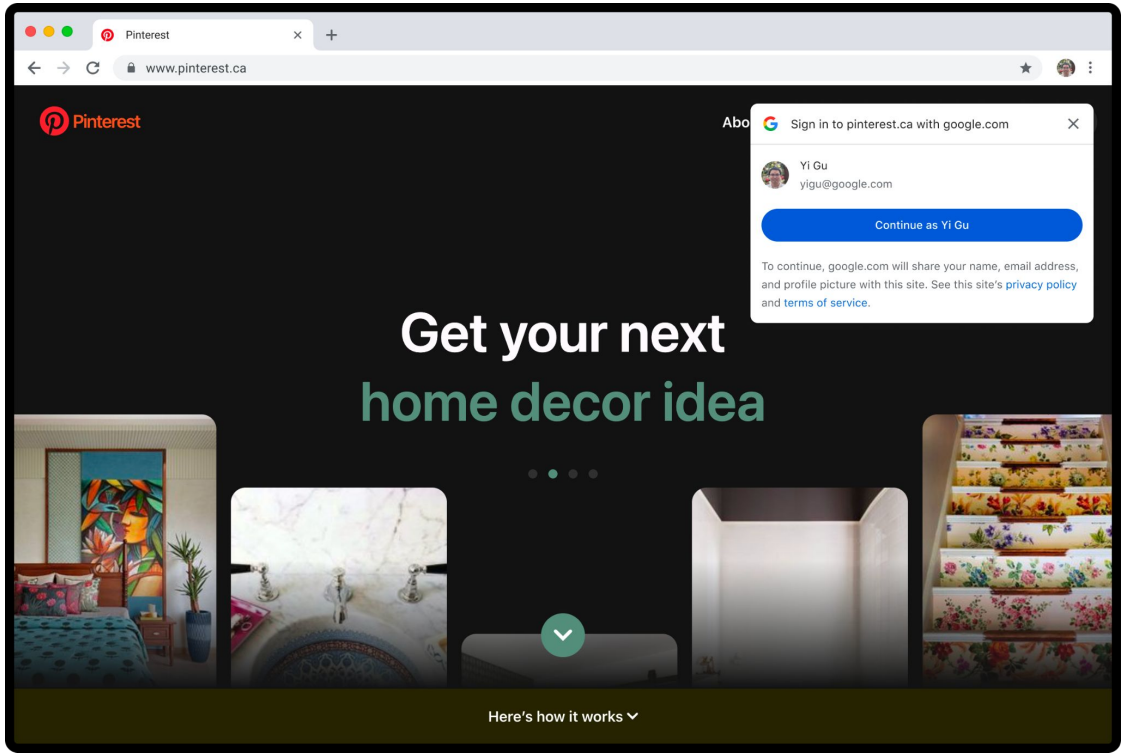
IDPs provide the verified claims in a privacy preserving manner (e.g. they don't learn where the claim is being used).





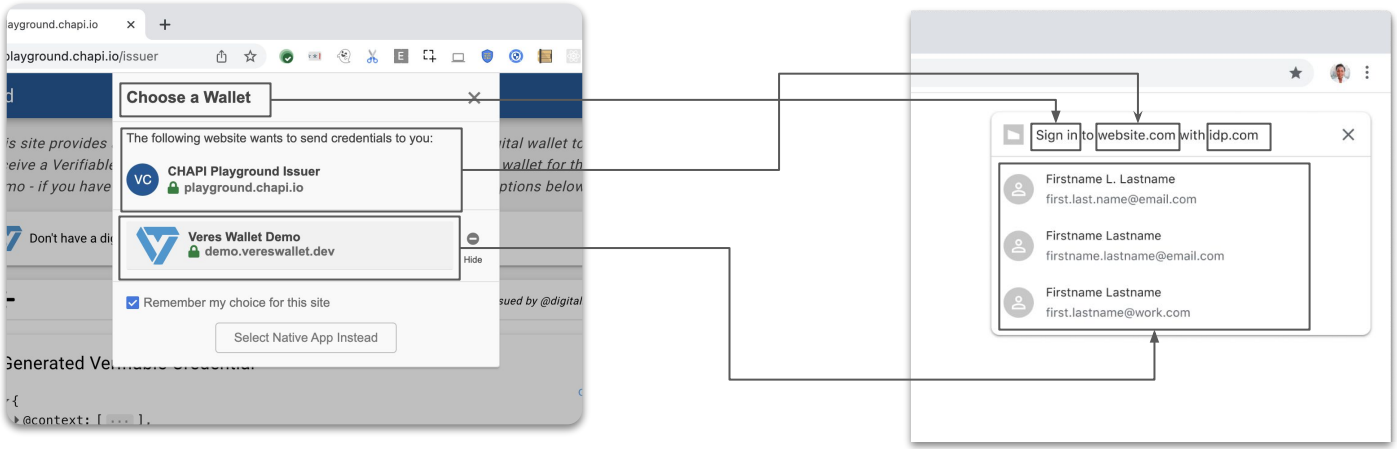
What are some shared interests?

Available publicly in chrome since M108



CHAPI

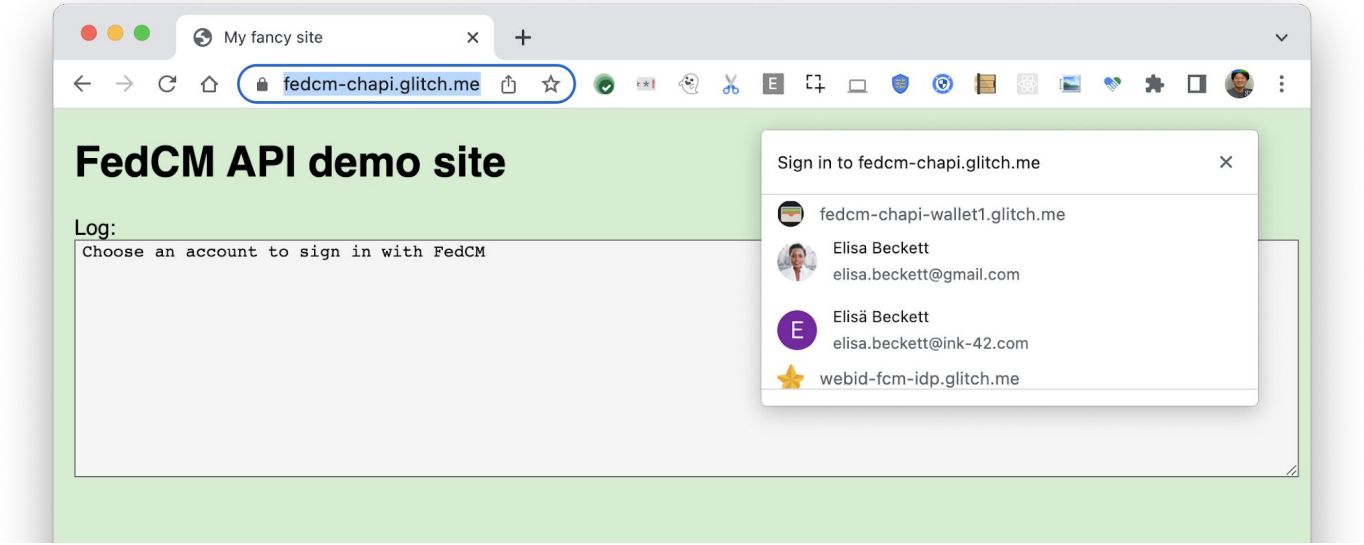
FedCM



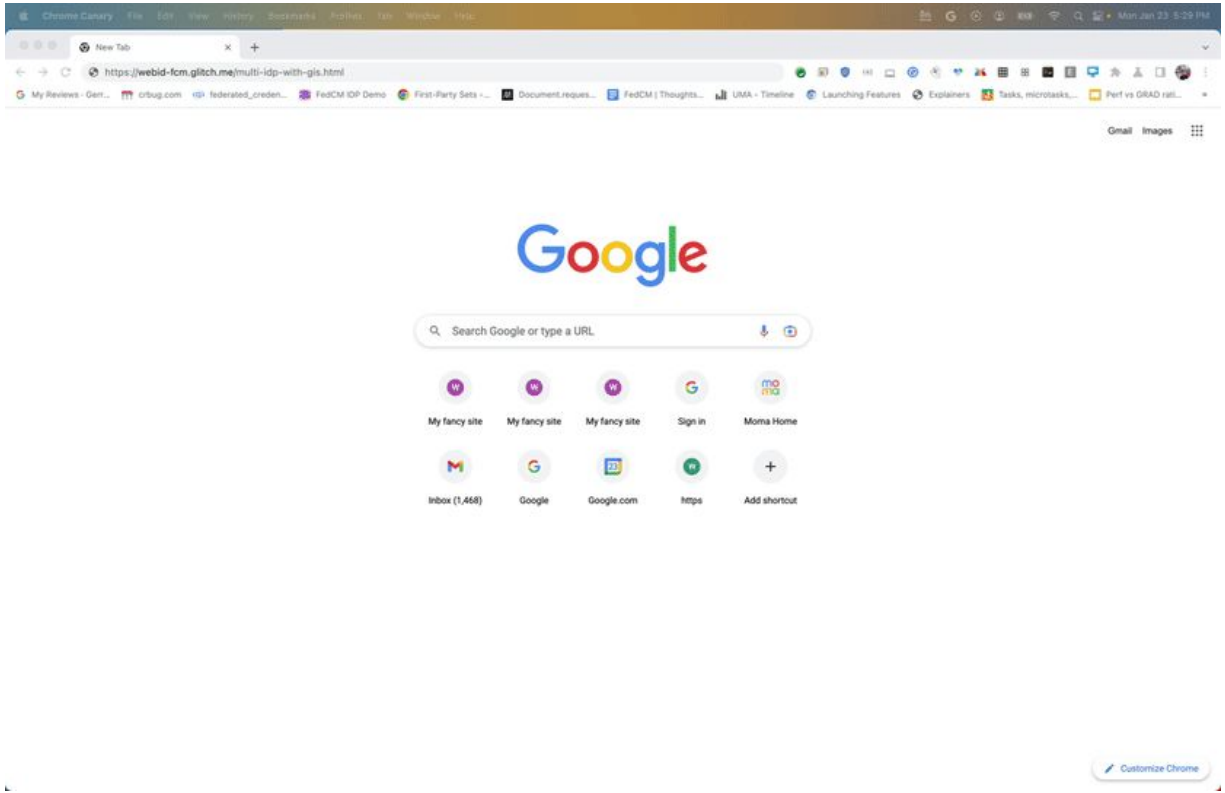
- Wallet Selector
- Multiple Wallets
- Wallet language
- Modal
- Wallet Registration
- Connects with Native Apps

- IdP Account Selector
- IdP Accounts from Single IdP
- Login language
- Non-modal
- IdP Selected by RPs
- Only cloud providers

The Multi IdP API



The Multi IdP API, also available behind a flag, allows you to add more than one IdP as a source of accounts to the UX prompt.
Here is an example of a prototype we built of a test wallet exposing itself as a FedCM IdP.


New Tab
https://webid-fcm.glitch.me/multi-idp-with-gis.html
Gmail
Images
Google
Search Google or type a URL
My fancy site
My fancy site
My fancy site
Sign in
Moma Home
Inbox (1,468)
Google
Google.com
https
Add shortcut
Customize Chrome

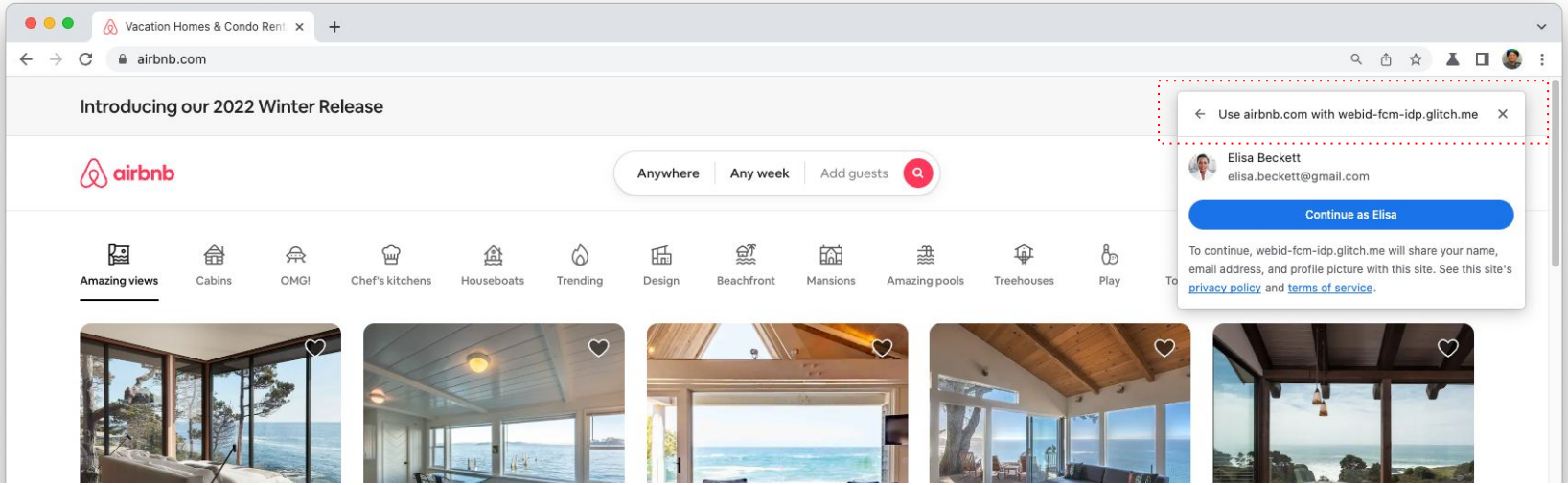
CHAPI

- Wallet Selector
- Multiple Wallets
- Wallet language
- Modal
- Wallet Registration
- Connects with Native Apps

FedCM

- IdP Account Selector
- IdP Accounts from ~~Single~~ Multiple IdP
- Login language
- Non-modal
- IdP Selected by RPs
- Only cloud providers

The RP Context API



The RP Context API, available behind a flag, allows you to use the FedCM prompt 4 different contexts: “use”, “continue”, “sign-up” and “sign-in”. I think this API may give us the expressivity to customize the UI to use the right language (e.g. control modality) for presentment and issuance of credentials.

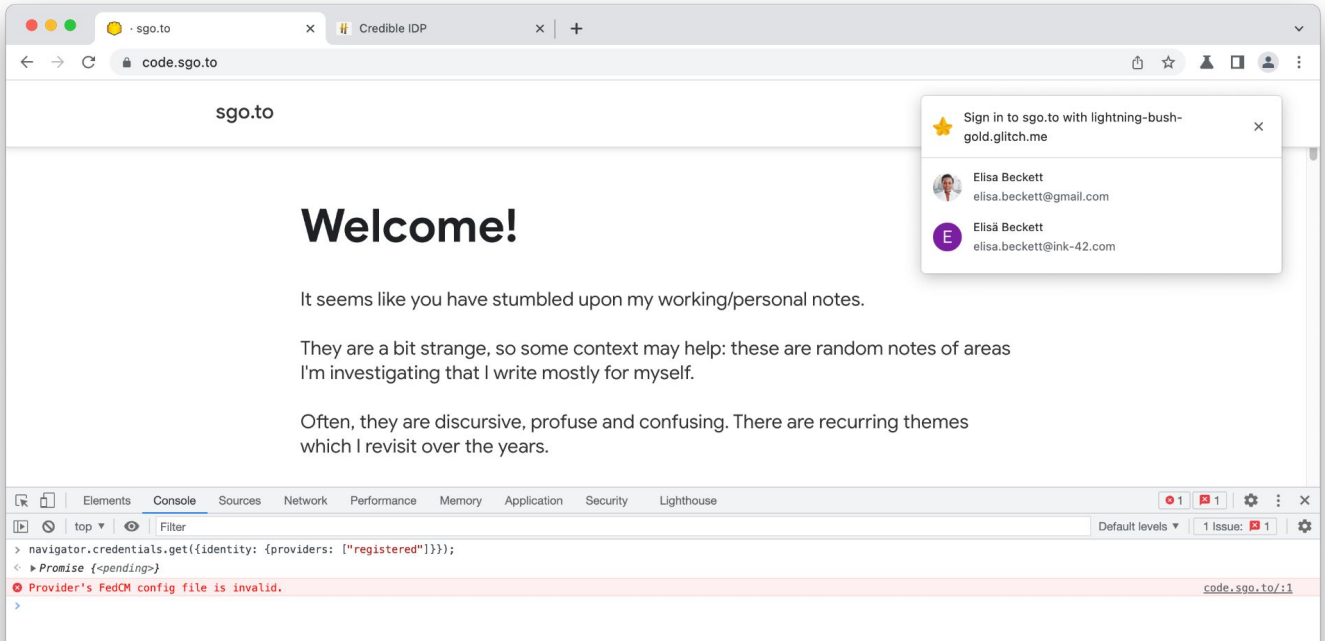
CHAPI

- Wallet Selector
- Multiple Wallets
- Wallet language
- Modal
- Wallet Registration
- Connects with Native Apps

FedCM

- ~~IdP~~ Wallet Account Selector
- ~~IdP~~ Wallet Accounts from ~~Single~~ Multiple ~~IdP~~ Wallets
- ~~Login~~ Wallet language
- ~~Non-modal~~
- ~~IdP~~ Wallet Selected by RPs
- Only cloud providers

The IdP Registry API



We built a small prototype of the IdP Registration API that would allow RPs to use IdPs that were registered before: IdentityProvider.register().
Somewhat comparable to navigator.registerProtocolHandler().

CHAPI

- Wallet Selector
- Multiple Wallets
- Wallet language
- Modal
- Wallet Registration
- Connects with Native Apps

FedCM

- ~~IdP~~ Wallet Account Selector
- ~~IdP~~ Wallet Accounts from ~~Single~~ Multiple ~~IdP~~ Wallets
- ~~Login~~ Wallet language
- ~~Non-modal~~
- ~~IdP~~ Wallet Registration ~~Selected by RPs~~
- Only cloud providers

CHAPI

- Wallet Selector
- Multiple Wallets
- Wallet language
- Modal
- Wallet Registration
- Connects with Native Apps

FedCM

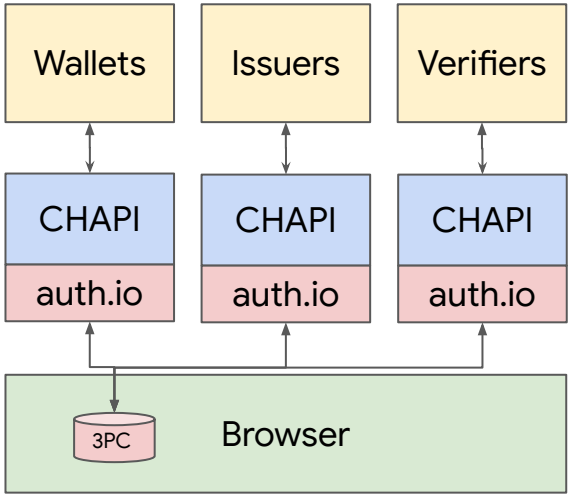
- Wallet Account* Selector
- Wallet Accounts* from Multiple Wallets
- Wallet language
- Modal
- Wallet Registration
- Only cloud providers (not covered, but easy)

I think there are going to be differences, but the bigger structural parts I think are similar enough.

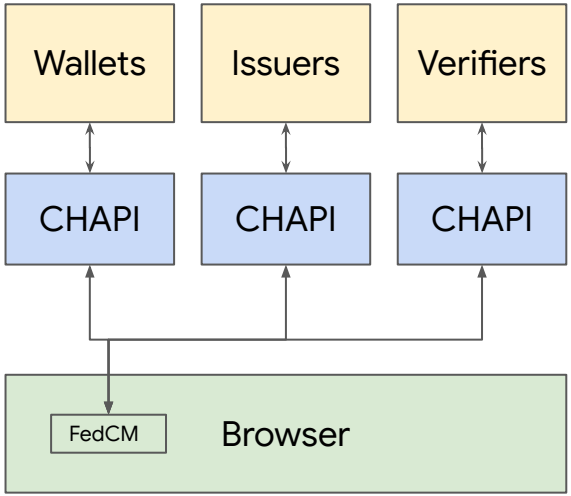
* I think you may call these “profiles” or “sessions”?

What if ...

Before

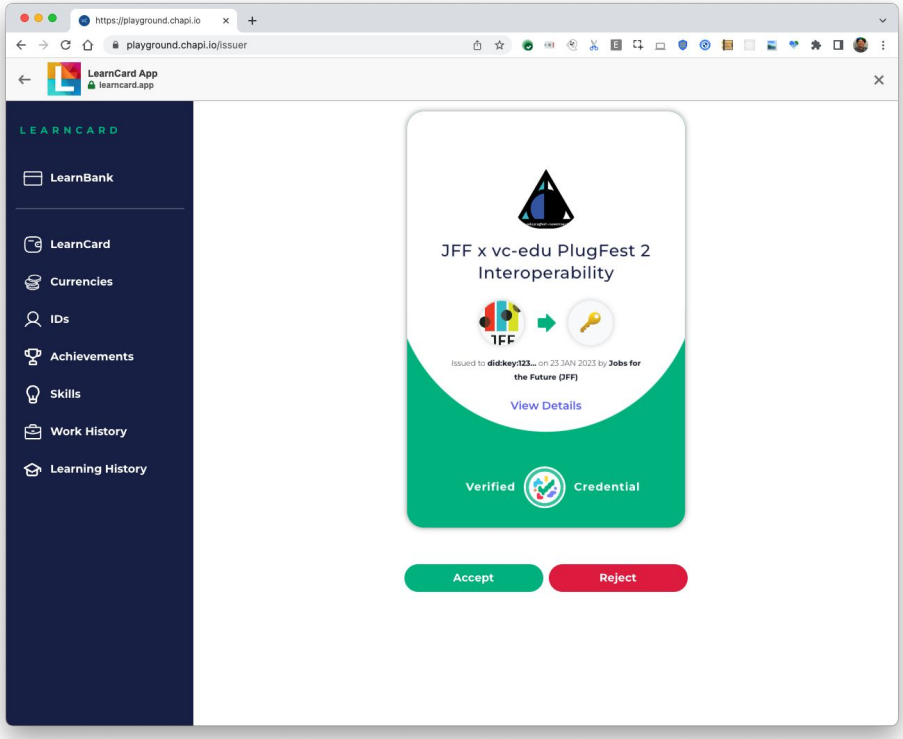


After

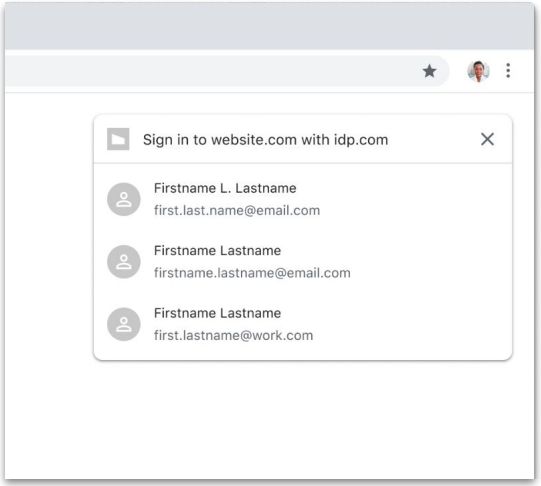


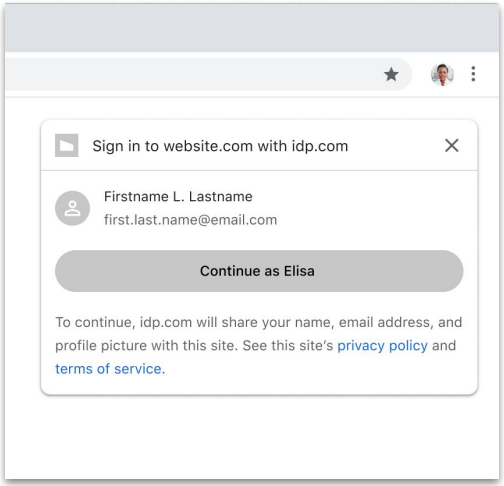
FedCM competes with cross-origin cookies / messaging, NOT with CHAPI. What I envision is CHAPI over FedCM, not FedCM in replacement of CHAPI. For example, it would be great if we could replace where you need auth.io with FedCM, but keep wallets/issuers and verifiers largely unaware of this transition, making it backwards compatible.

Awkward parts ...

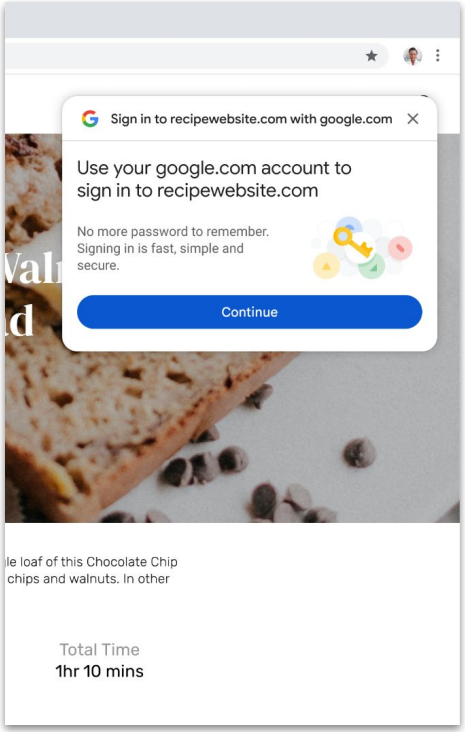


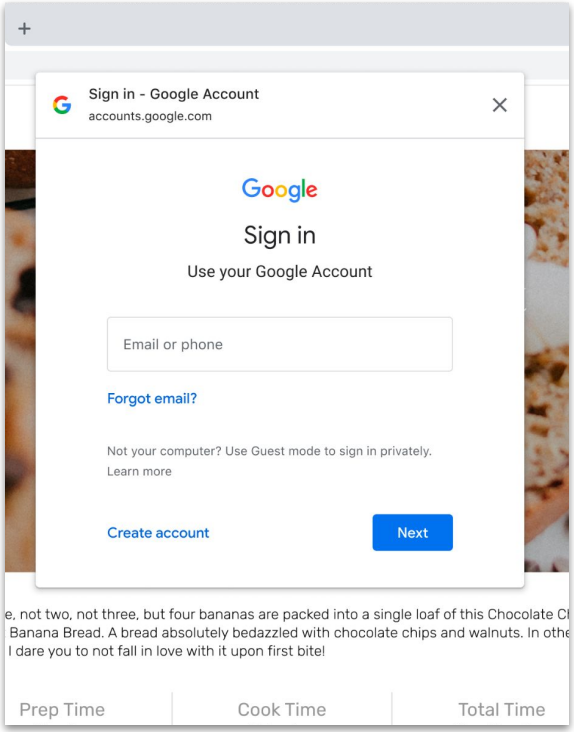
In this UX here, CHAPI delegates rendering to Wallets, which doesn't yet exist in FedCM.
We'd have to go through a good amount of Privacy/Security analysis here to enable something like this.
I don't think this is a non-starter, but wanted to flag early where we may run into a wall.

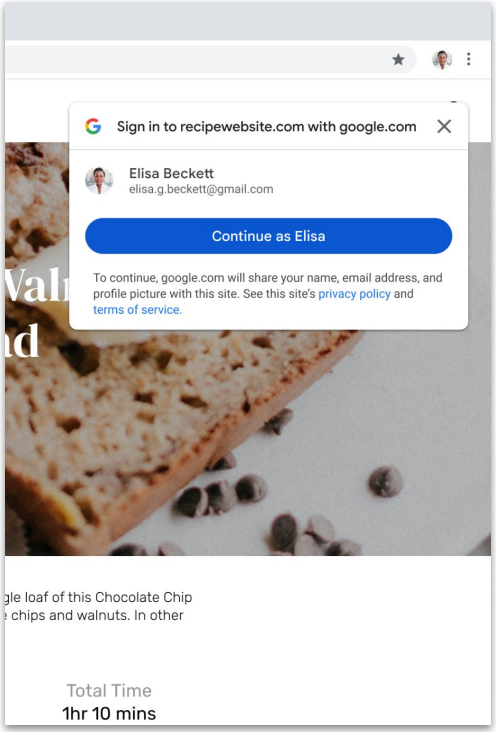

Sign in to website.com with idp.com
Firstname L. Lastname
first.last.name@email.com
Firstname Lastname
firstname.lastname@email.com
Firstname Lastname
first.lastname@work.com


Sign in to website.com with idp.com
Firstname L. Lastname
first.last.name@email.com
Continue as Elisa
To continue, idp.com will share your name, email address, and profile picture with this site. See this site's privacy policy and terms of service.

The IdP Sign-in UX







The closest we have to the Wallet presentment/issuance UI is what we are building to introduce the ability for the user to sign-in to the IdP. This is a pop-like UI that loads the IdP in a first party context.

Overall, it is still unclear to me if CHAPI over FedCM is (a) possible and / or (b) desirable.

There are more questions than answers at this point.

But, I do think it is worth giving a it a try: I think (a) we agree more than we disagree, (b) we are working on similar problems and (c) and we would learn/benefit from each other.

WDYT?

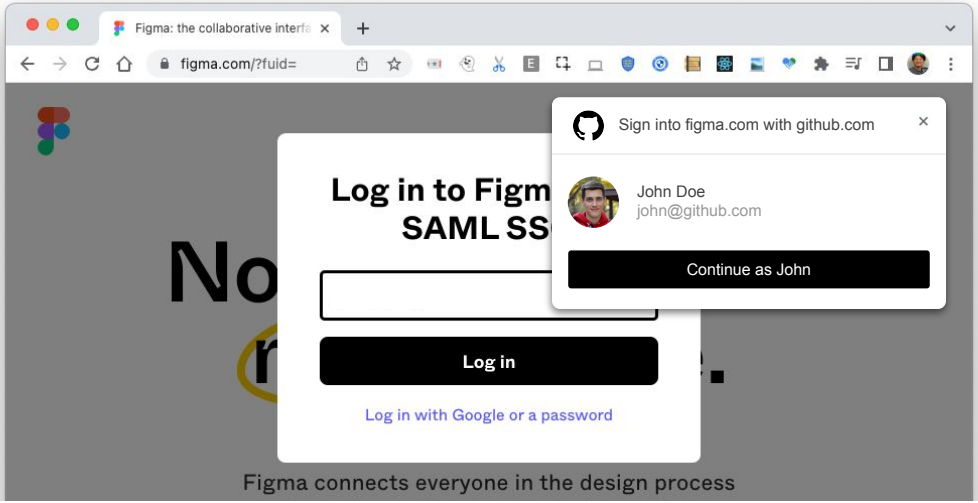
GC

Prototypes

Illustrative Mock
NOT ready to build

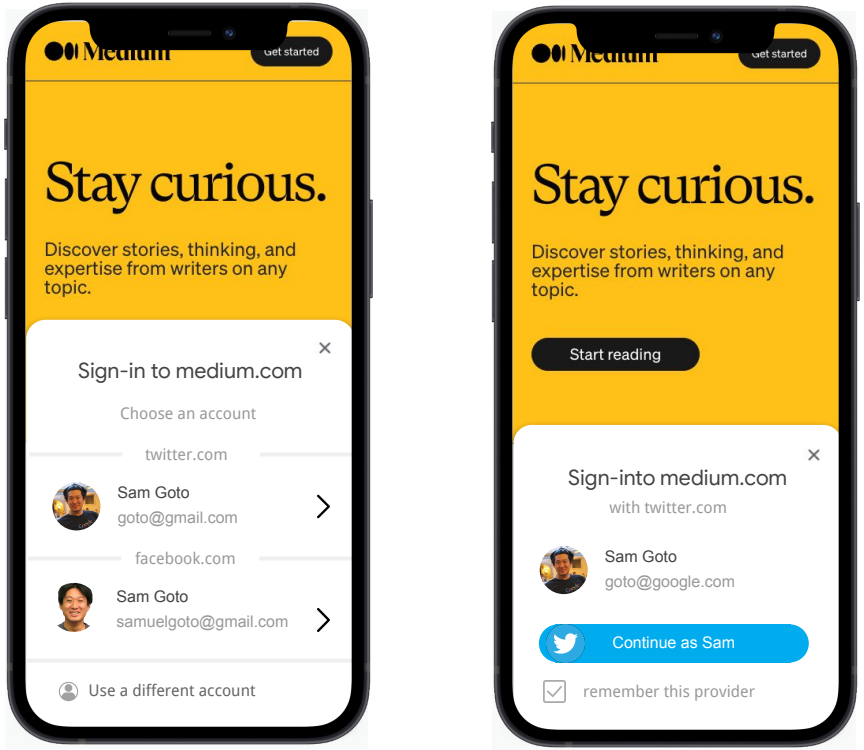
Employee IDs

Issue #62



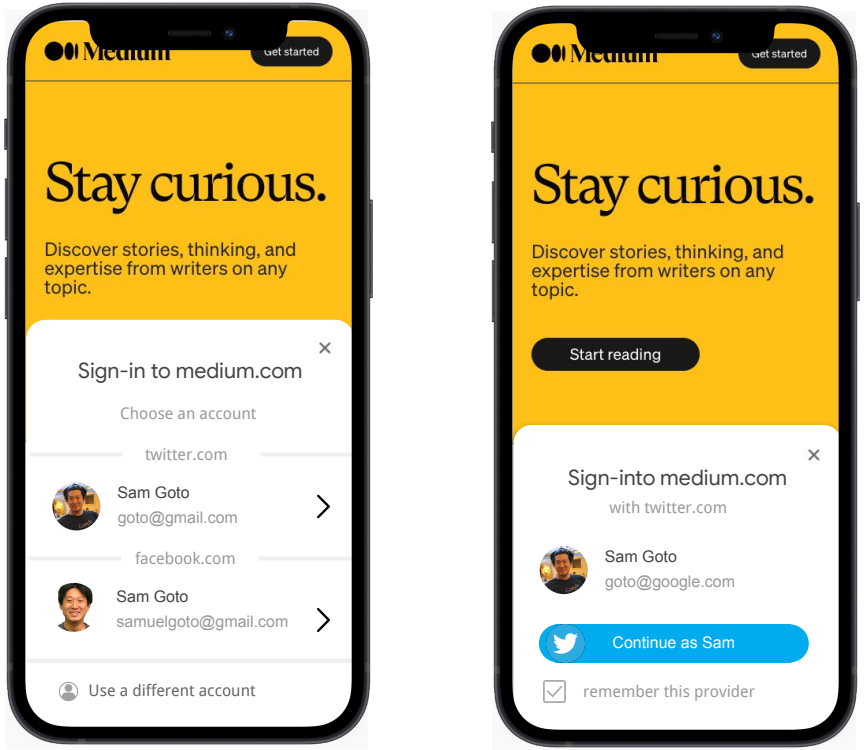
A few other awkward situations: service workers, etc.

Early Mocks



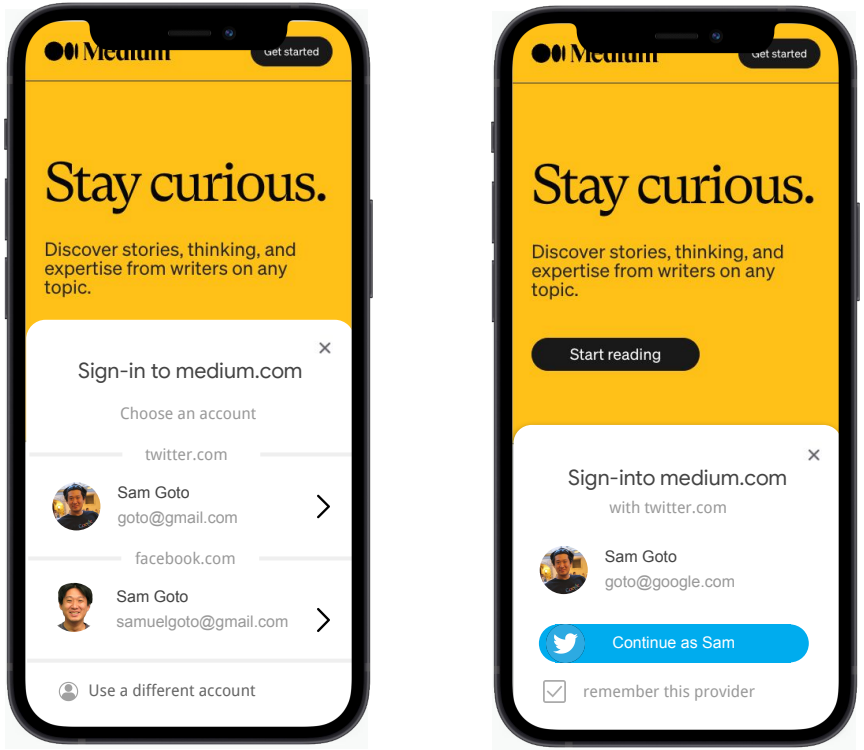
FedCM mediates account choosing **and** information sharing.
It is NOT a general purpose cross-site communication channel: it exchanges identities.

Early Mocks



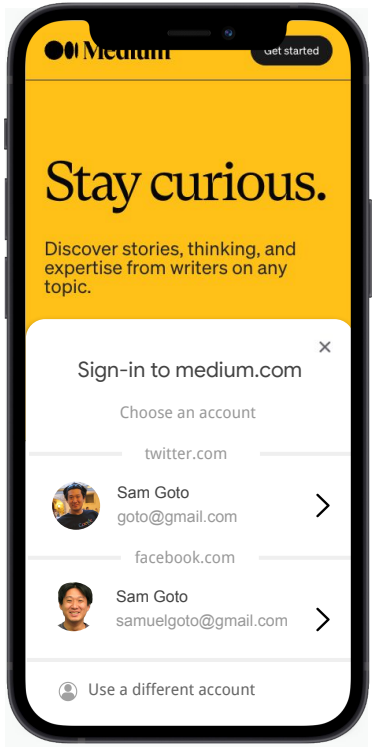
FedCM gathers the user's consent **on behalf of** the IdP.

Early Mocks



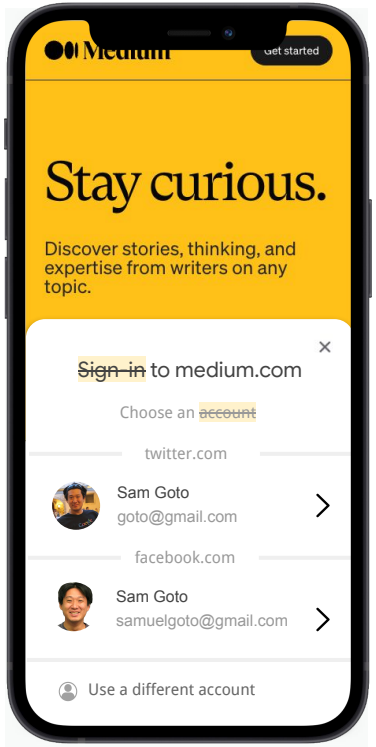
That leads to a trade-off between IdP expressivity / extensibility and user control / aggregation. There isn't right or wrong, but we started with something constrained / narrow rather than general / broad.

Early Mocks



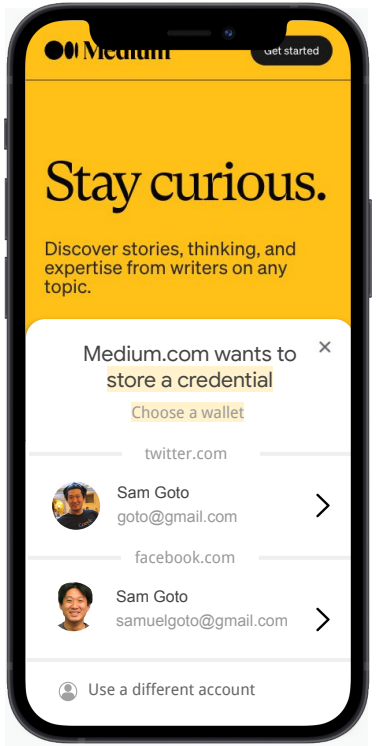
So, let's start with FedCM's Multiple IdP account chooser as a baseline.

Early Mocks

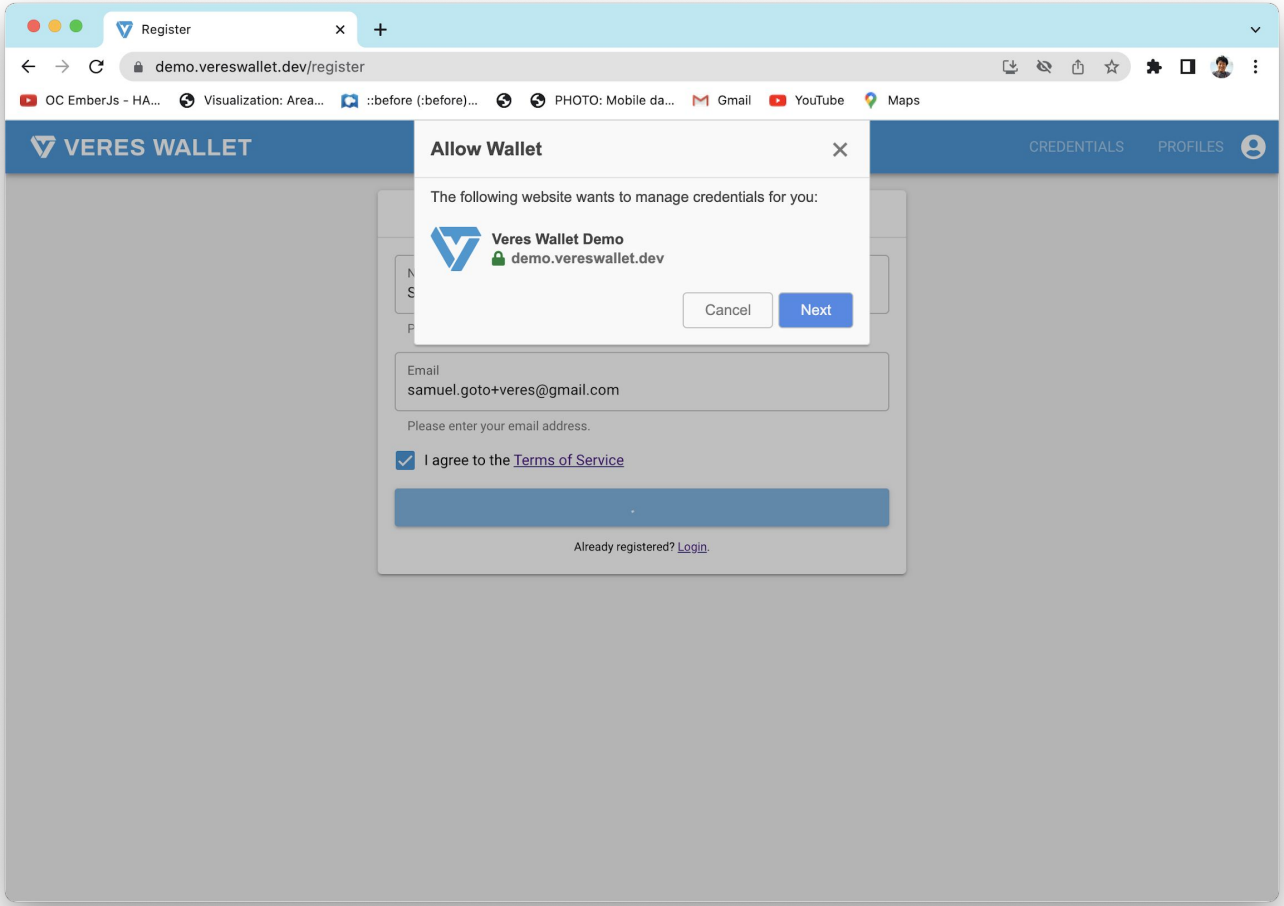


First, let's get rid of these sign-in preconceptions.

Early Mocks

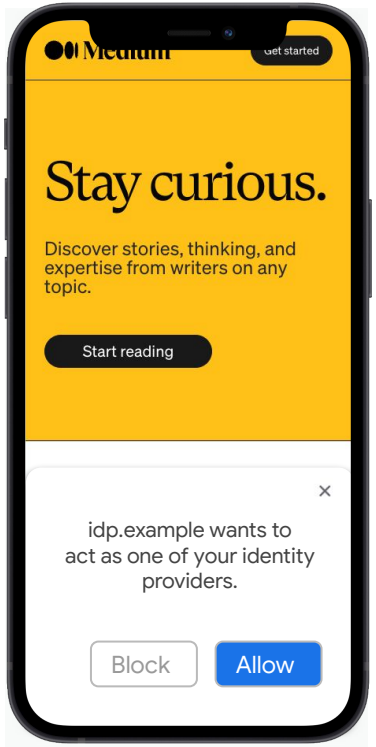


Ok, that seems better.



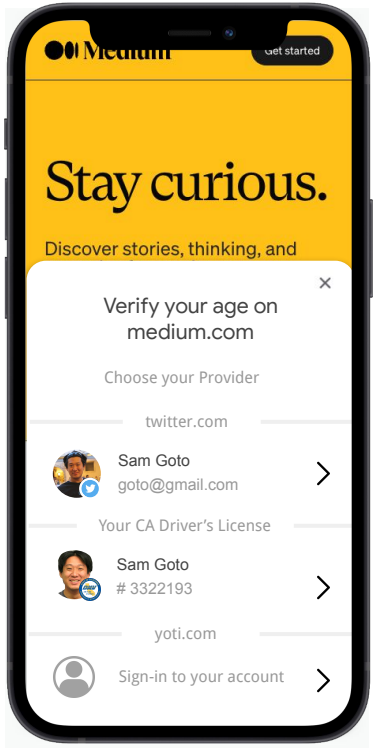
Second, CHAPI allows Wallets to be registered as opposed to named.

Early Mocks



And the IdP registration API should allow users to bring their own identities to sites.

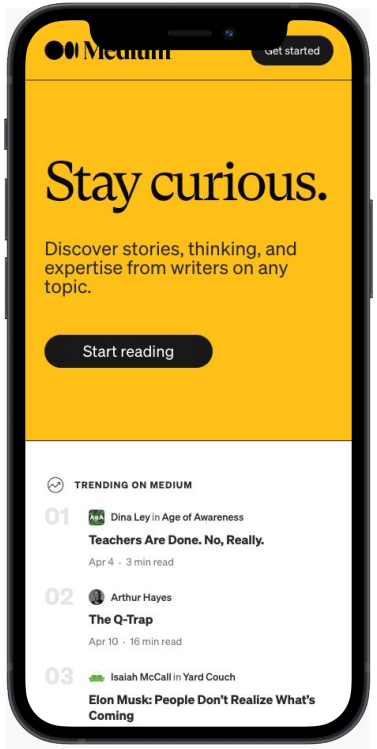
Early Mocks

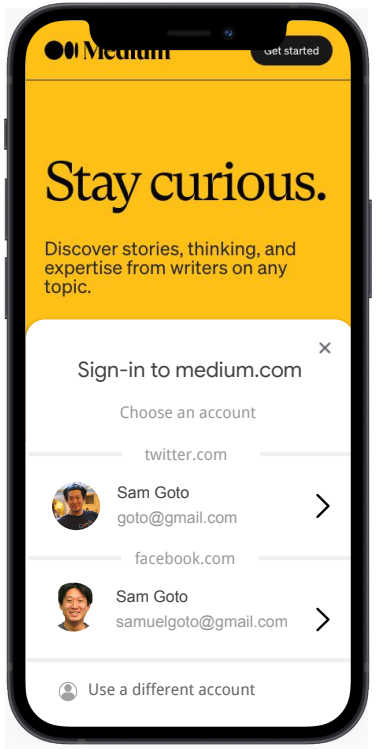


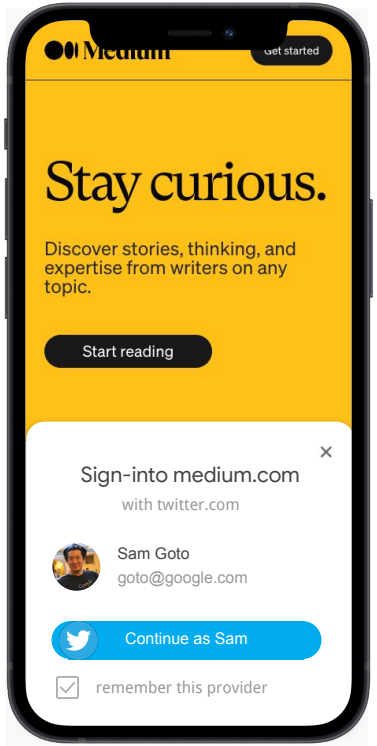
CHAPI seems to be able to connect with native wallets. I think, as a lower layer, browsers can do better.

Early Mocks

Single attributes (account), single issuer type (federated), multiple providers (twitter/facebook)

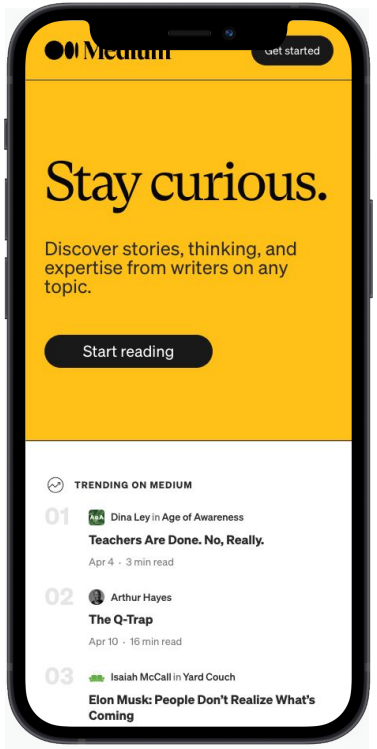


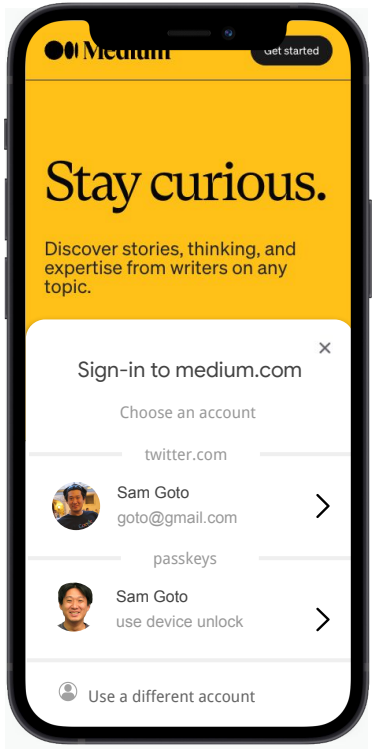


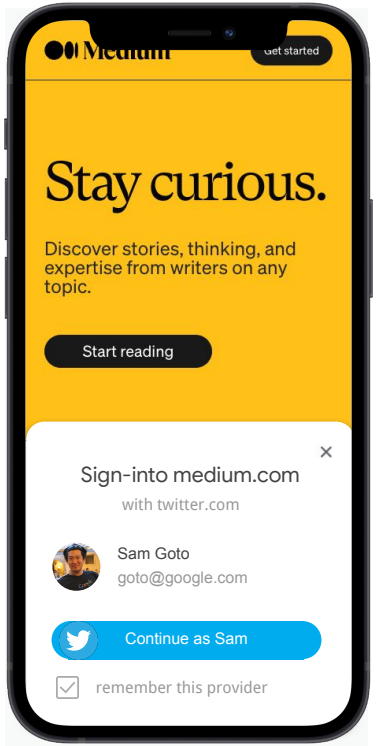


Early Mocks

Either-or-Multiple attributes (account OR passkey), multiple issuer type (publicKey, federated), multiple providers (twitter/facebook + yubico)

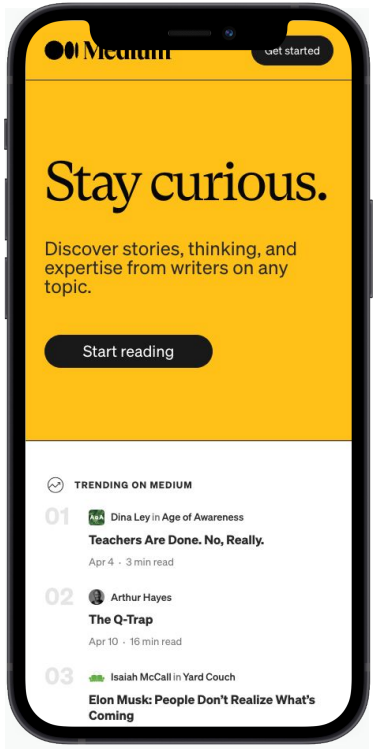


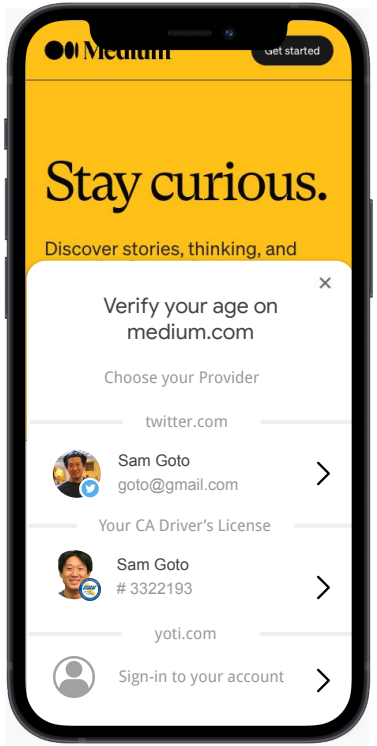


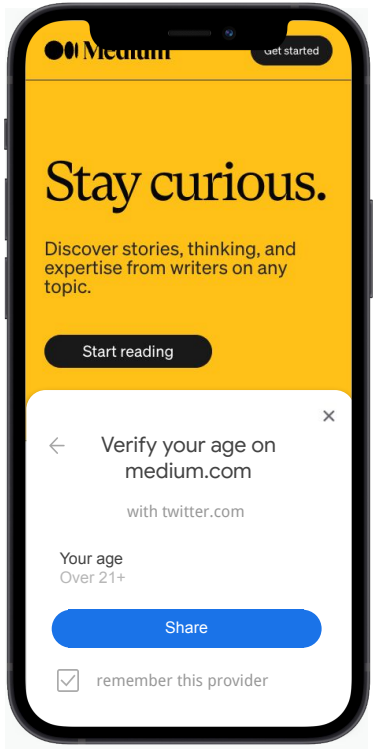


Early Mocks

Single attributes (age bracket), multiple issuer type (federated and mDLs), multiple providers (twitter and the DMV)

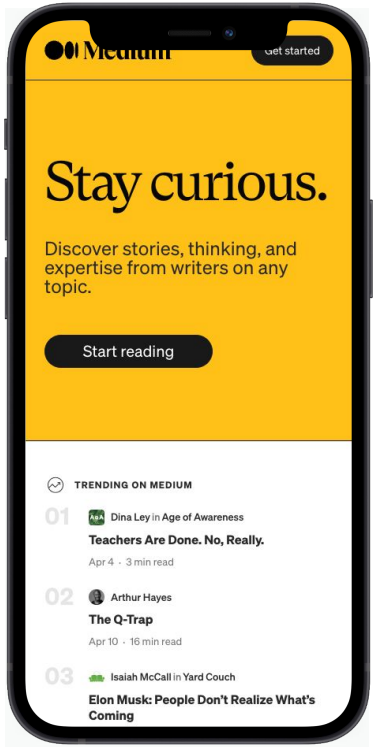


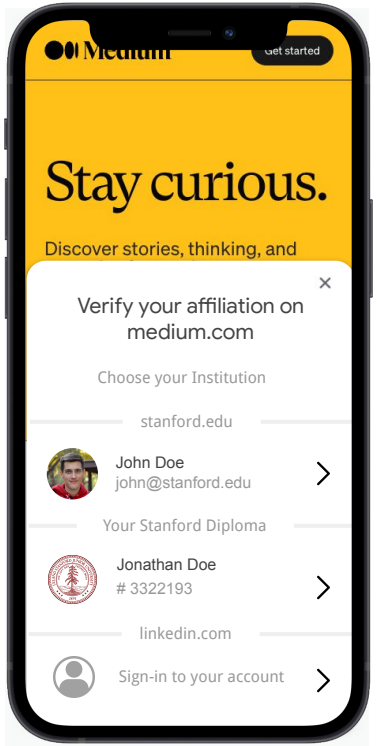


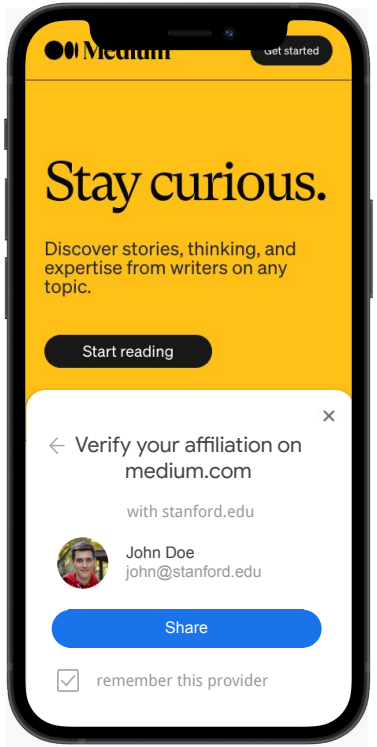


Early Mocks

Single attributes (age bracket), multiple issuer type (federated and VCs), multiple providers (stanford.edu and a locally available diploma)







Use case: a scientific article in a journal is restricted to university students.