# FedCM Update

## where we are and where we are going

yigu@chromium.org cbiesinger@chromium.org

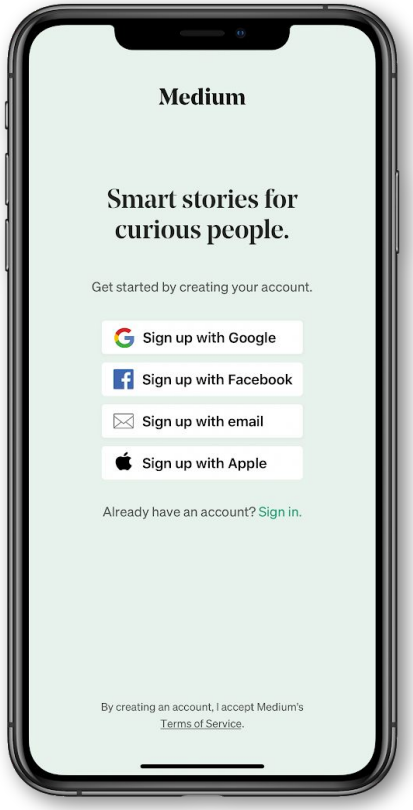
# Why Federated Credentials?

**What is it?**

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

**Why do we think it's important?**

- Ease of use
  - passwordless
- Security
  - resistance to phishing
- Trustworthiness
  - per-site username and password



# The problem

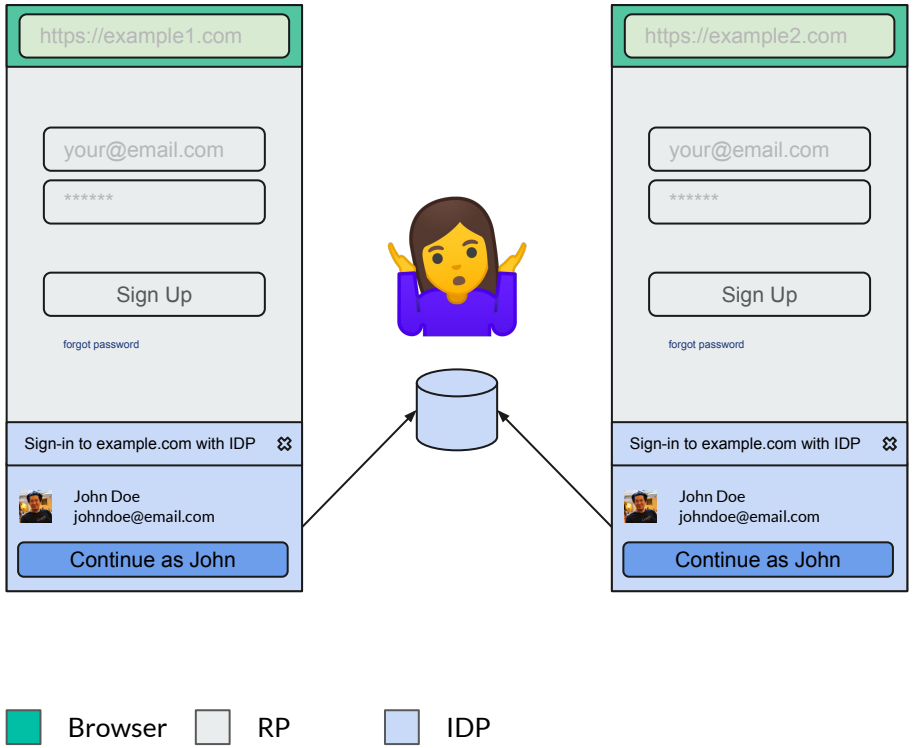
By design, identity federation was built on top of low-level primitives*.

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

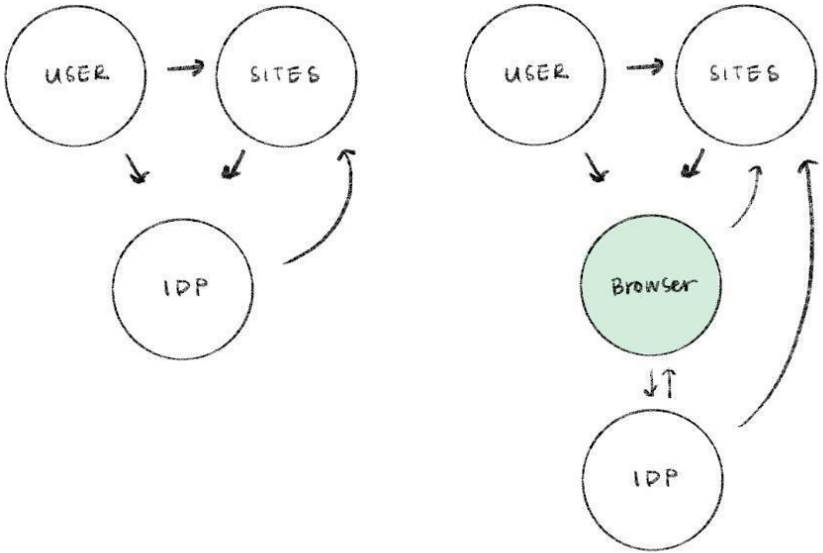
Unfortunately, we can't distinguish tracking from federation.

* iframes, third party cookies, redirects

## The classification Problem



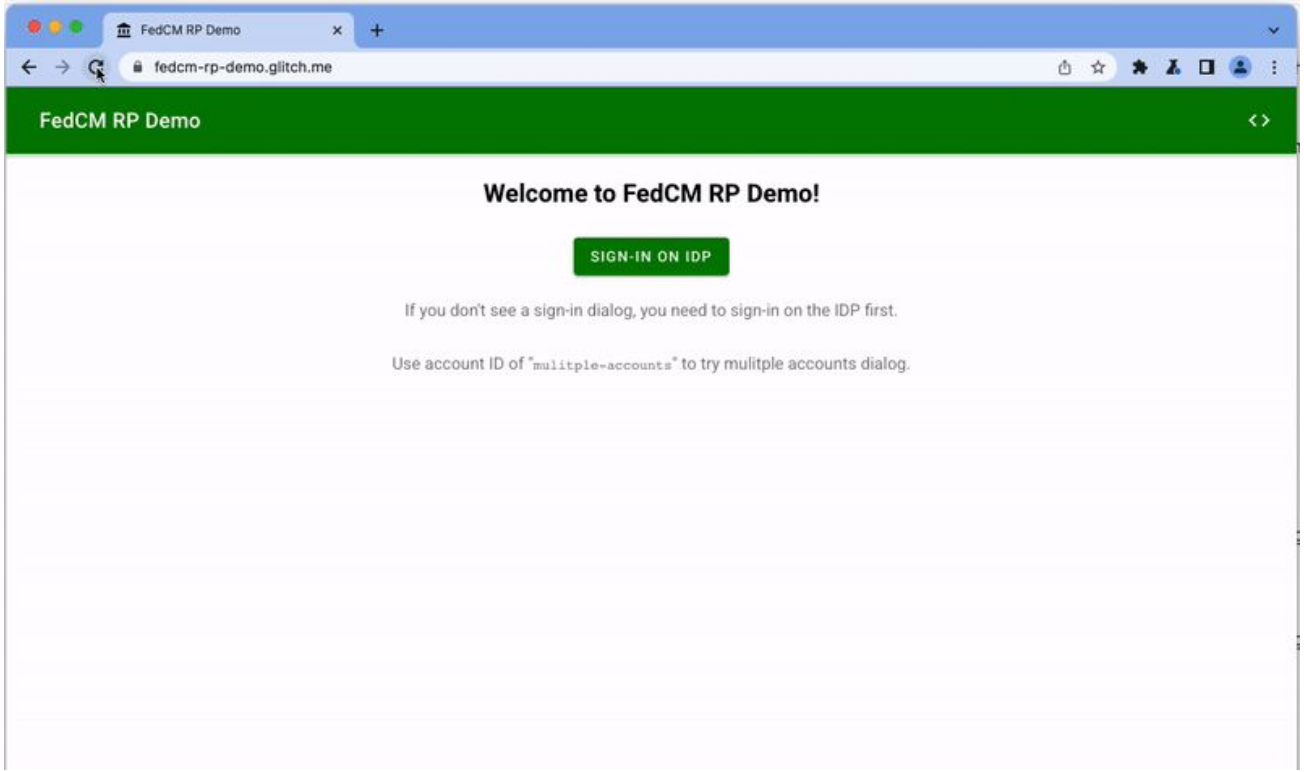
# How?



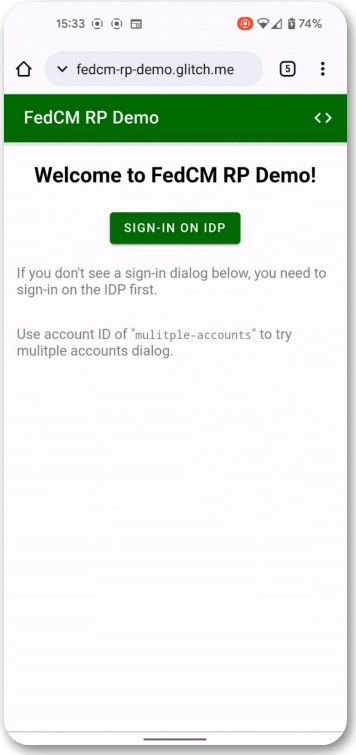
# How?

| O(10s) | O(100s) | O(M) | O(B) |
| --- | --- | --- | --- |
| Browsers | Identity Providers | Relying Parties | Users |
| Heavy change | Moderate change | Backwards compatible | No behavioral changes |

# Demo time!


FedCM RP Demo
fedcm-rp-demo.glitch.me
FedCM RP Demo
Welcome to FedCM RP Demo!
SIGN-IN ON IDP
If you don't see a sign-in dialog, you need to sign-in on the IDP first.
Use account ID of "mulitple-accounts" to try mulitple accounts dialog.

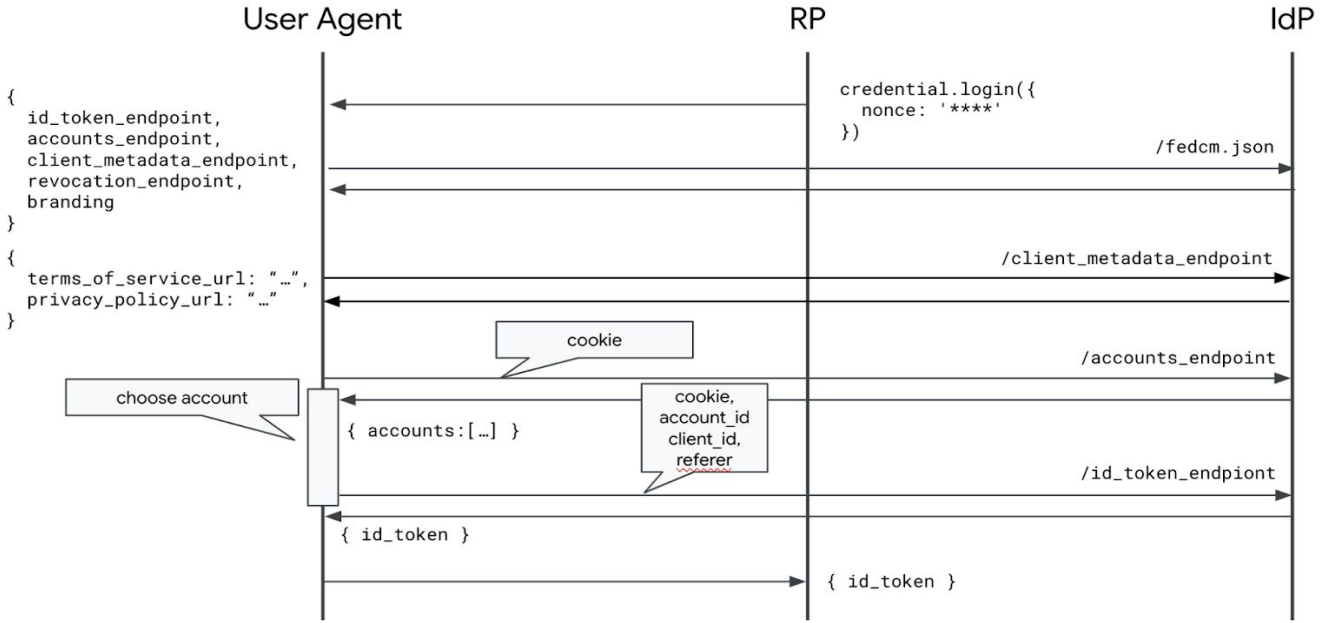
# Demo time!


15:33
74%
fedcm-rp-demo.glitch.me
FedCM RP Demo
Welcome to FedCM RP Demo!
SIGN-IN ON IDP
If you don't see a sign-in dialog below, you need to sign-in on the IDP first.
Use account ID of "mulitple-accounts" to try mulitple accounts dialog.

# How? The JavaScript API

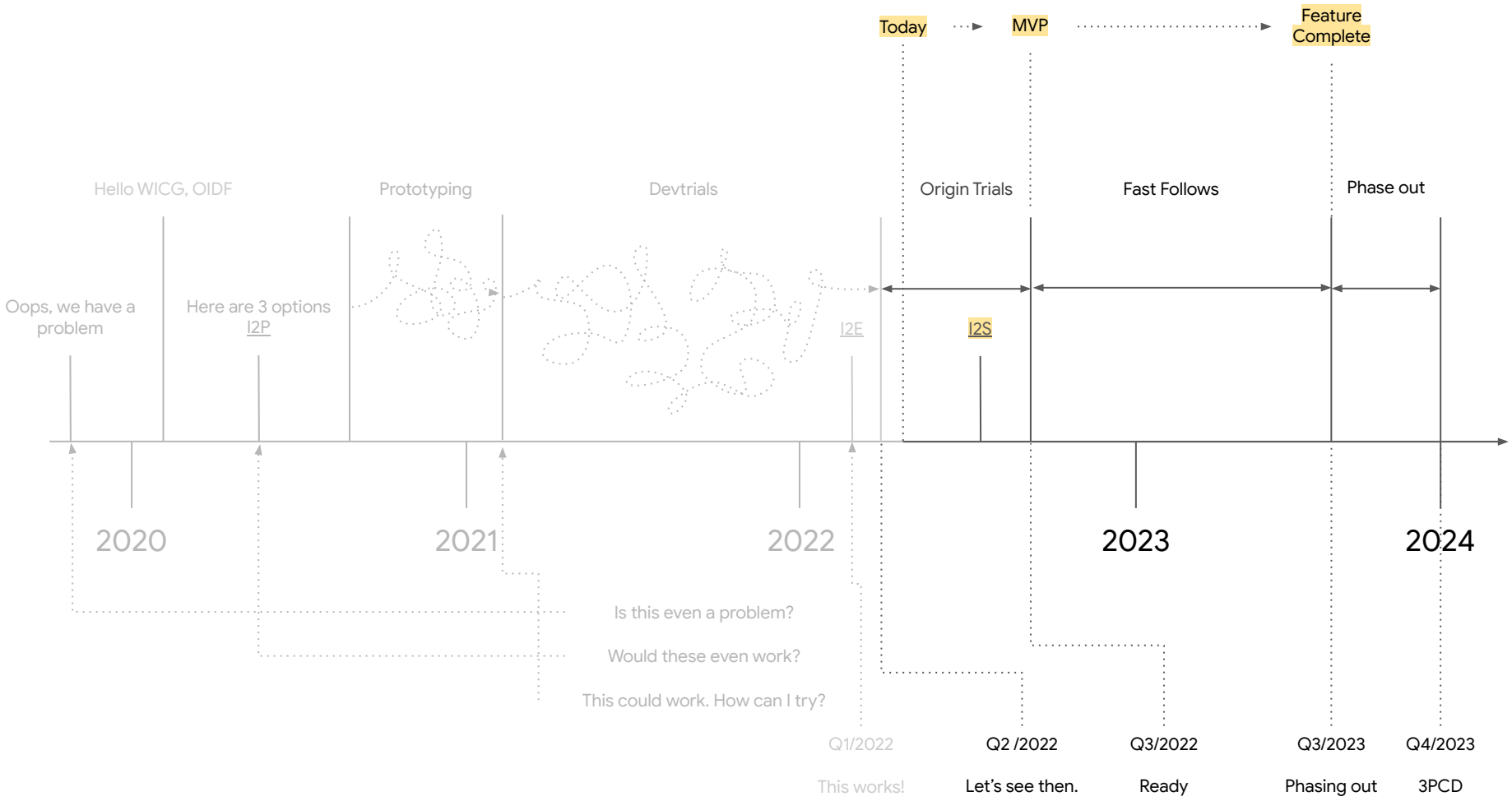
```
var credential = navigator.credentials.get(
    {provider: "https://idp.example/", client_id: "123"} );
{id_token} = credential.login();


// Also available:

credential.logout();
credential.revoke();
```

# How? The HTTP API




https://developer.chrome.com/blog/fedcm-origin-trial/

# When?

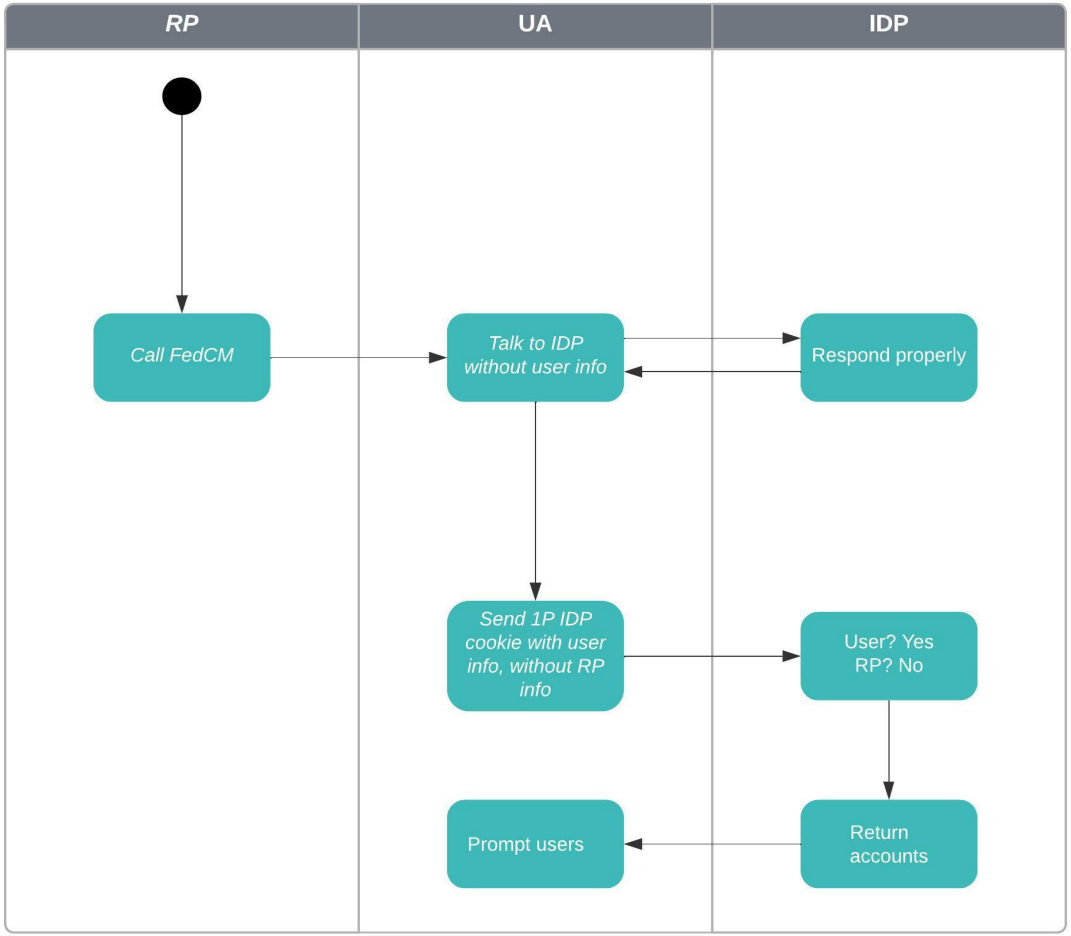

Today
MVP
Feature Complete
Hello WICG, OIDF
Prototyping
Devtrials
Origin Trials
Fast Follows
Phase out
Oops, we have a problem
Here are 3 options
I2P
I2E
I2S
2020
2021
2022
2023
2024
Is this even a problem?
Would these even work?
This could work. How can I try?
Q1/2022
Q2 /2022
Q3/2022
Q3/2023
Q4/2023
This works!
Let's see then.
Ready
Phasing out
3PCD

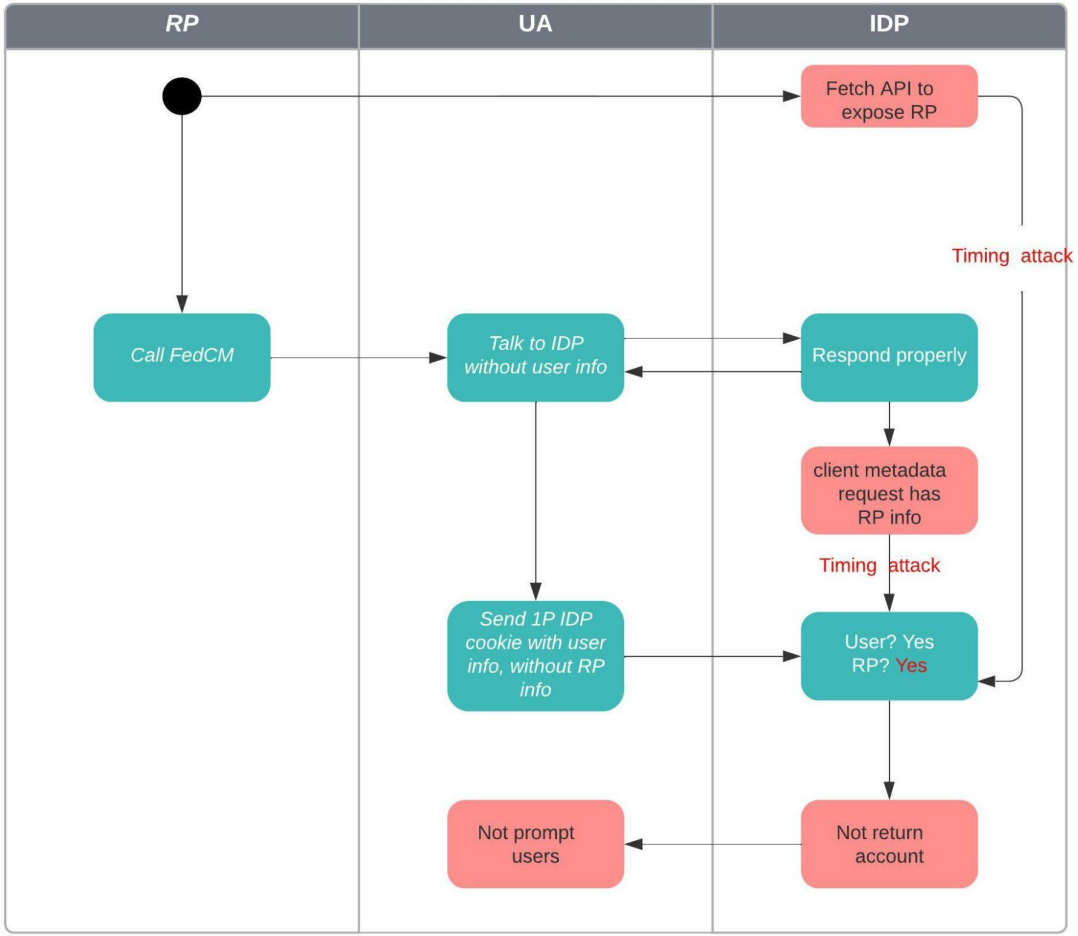
# Ecosystem Feedback

- Federated Identity Community Group
- Identity Providers
  - Better understanding of the use cases (primitives by use cases)
    - Firmer validation that front-channel logout is important to them
  - Better understanding of the alternatives and trade-offs (alternatives considered)
    - First Party Sets, CHIPS, Storage Access API, FedCM, CNAMES, Back channel logout, etc.
  - Increasingly more concerned about bounce tracking mitigations longer term
- Browsers
  - Edge: no institutional position yet. currently running the origin trial too.
  - Safari: early institutional position: generally supportive, but still very early / shallow
  - Firefox: no institutional position yet. informally, supportive of development, concerned about a few privacy issues which we are working on together.

# The Timing Attack

- Tracker can learn about which website a user is visiting without user permission by conducting the timing attack


RP
UA
IDP
Call FedCM
Talk to IDP without user info
Respond properly
Send 1P IDP cookie with user info, without RP info
User? Yes
RP? No
Prompt users
Return accounts


RP
UA
IDP
Fetch API to expose RP
Timing attack
Call FedCM
Talk to IDP without user info
Respond properly
client metadata request has RP info
Timing attack
Send 1P IDP cookie with user info, without RP info
User? Yes
RP? Yes
Not prompt users
Not return account

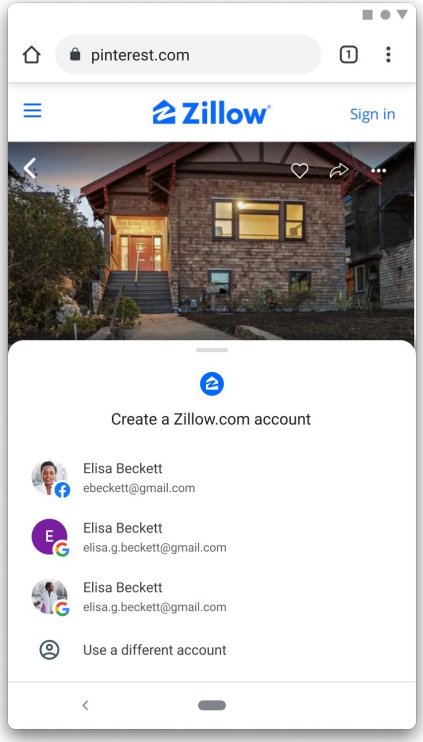
# Proposal - pull accounts iff it’s necessary

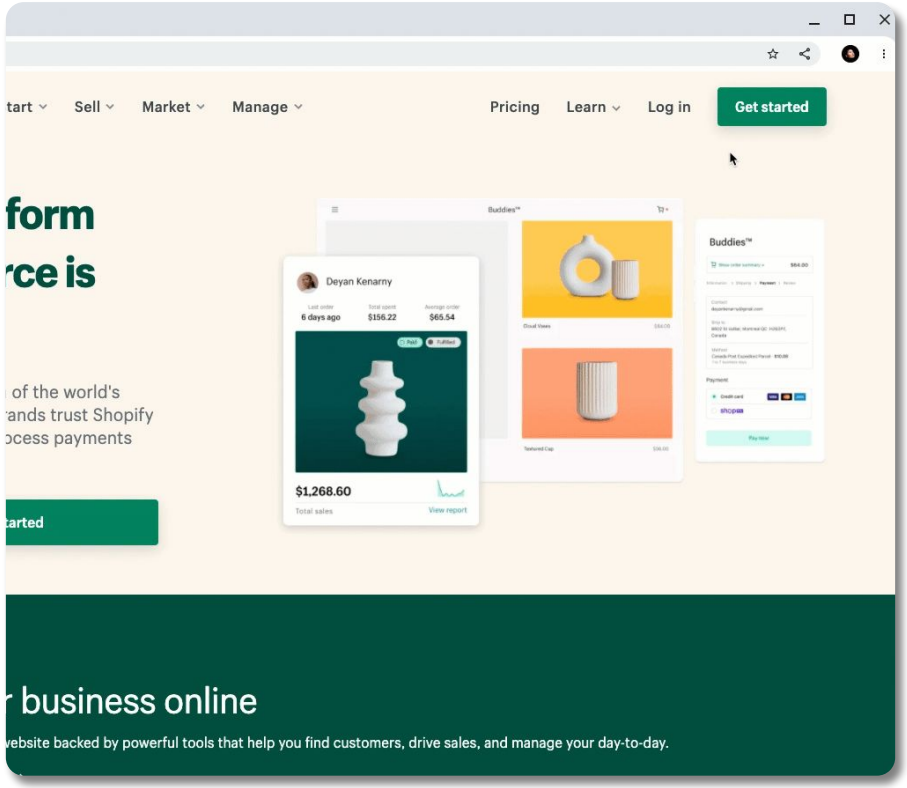
- Site engagement score: users must have interacted with the provider origin in the past
  - { provider: “**https://idp.example/**”, client_id: “123” }
- Aggregate metrics to penalize suspicious “providers”
  - Click-through rate
  - Invisible UI rate

- We want the timing attack to be economically impractical, not mathematically impossible

# What’s next: Multiple IDPs?

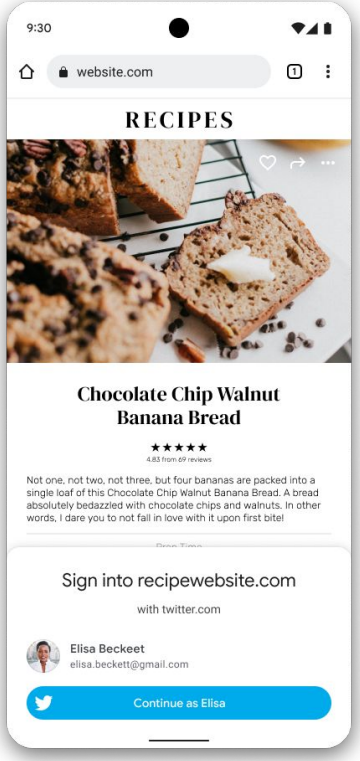
Company logos are illustrative only

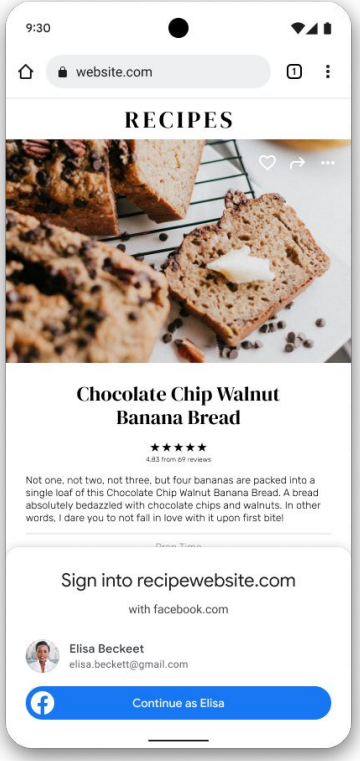


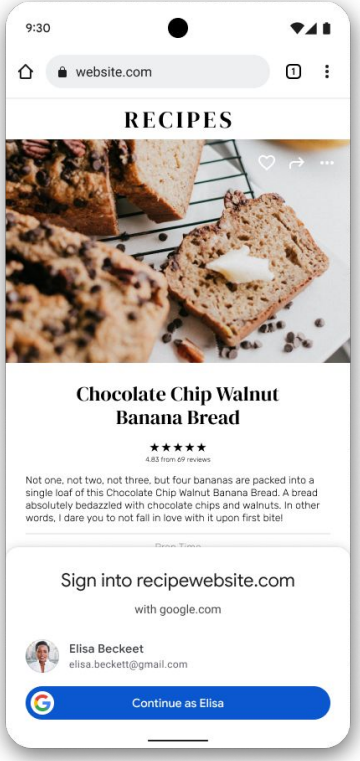



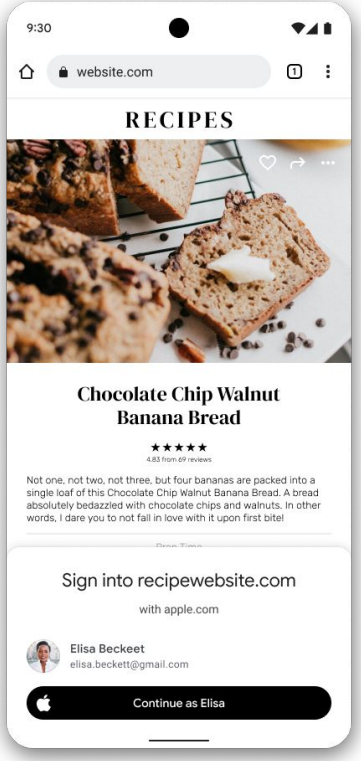
# What’s next: Branding?

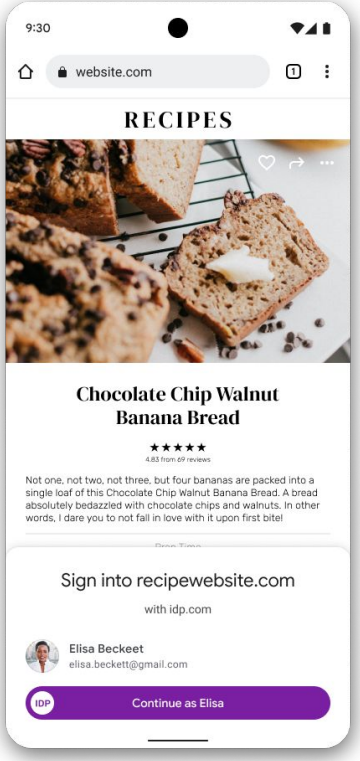
Company logos are illustrative only



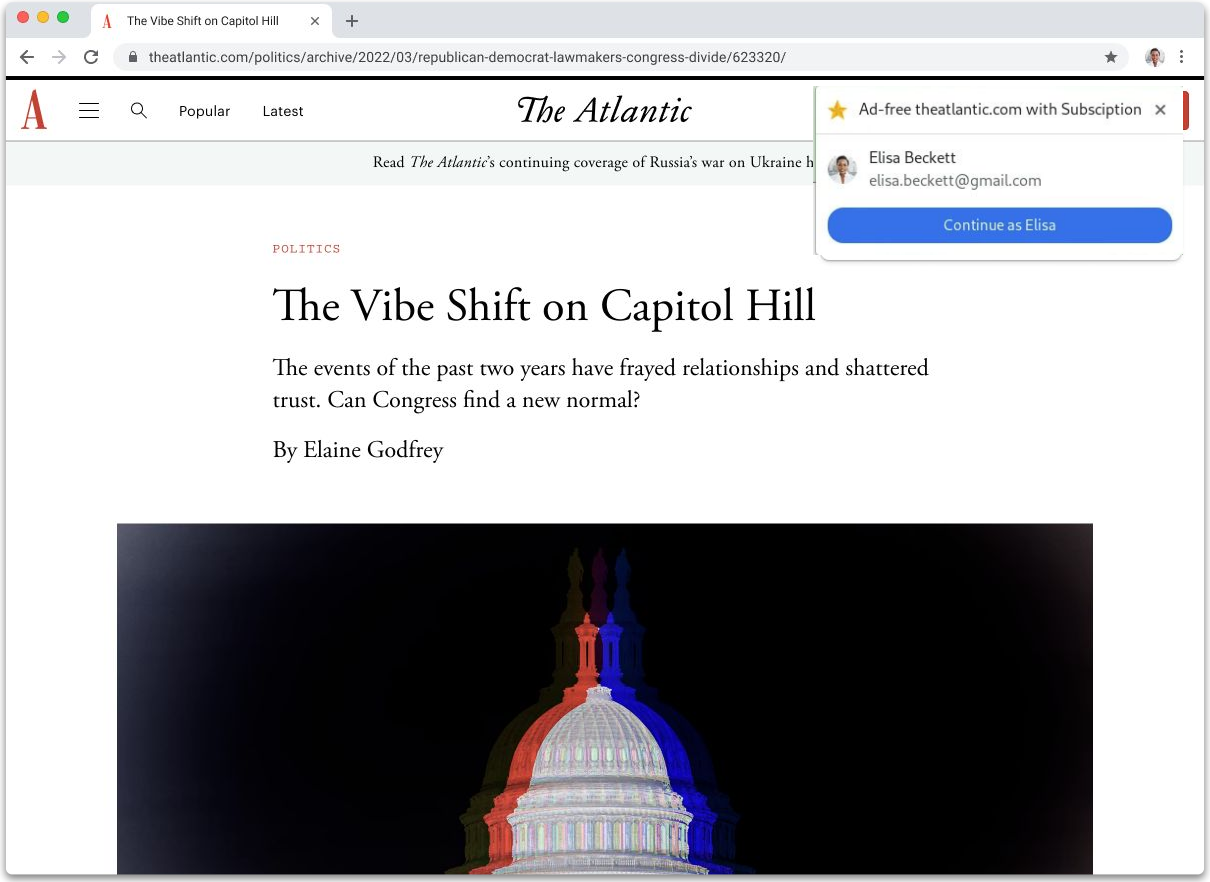



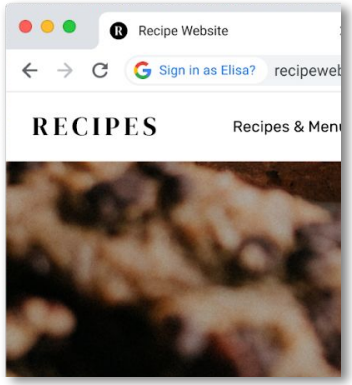
# What's next: Other Use Cases?

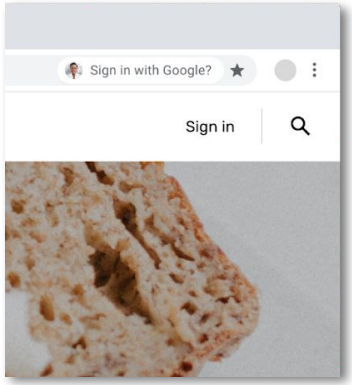
Company logos are illustrative only

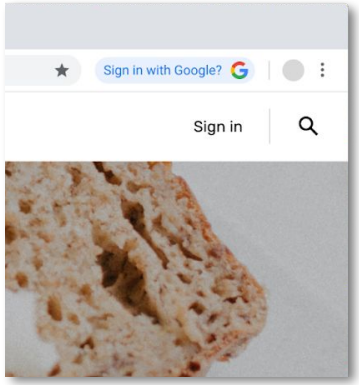


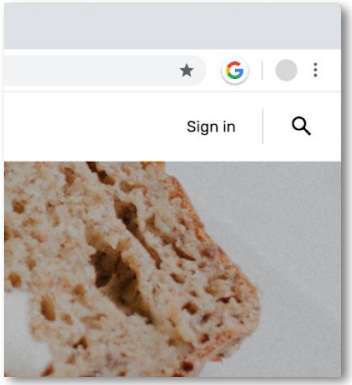
# What’s next: previously inaccessible UX opportunities?

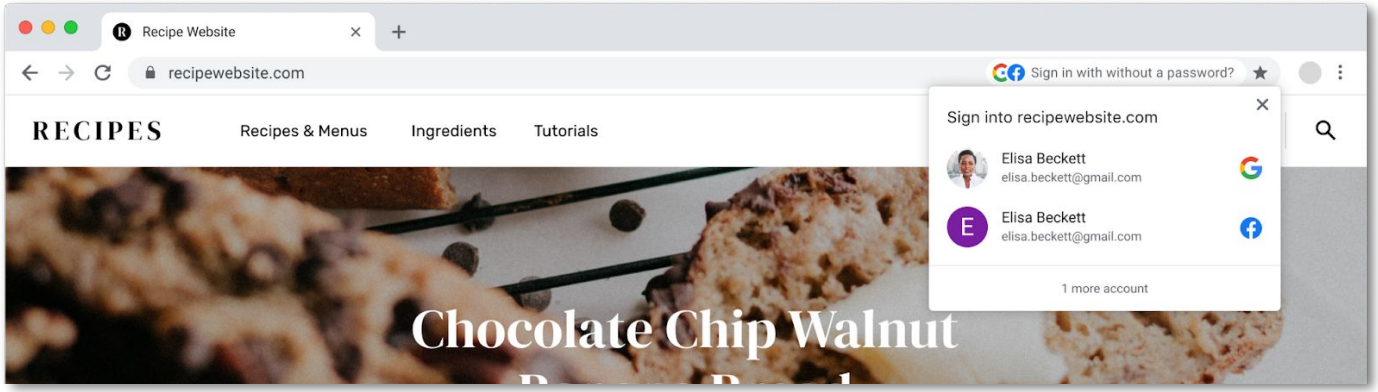
Company logos are illustrative only



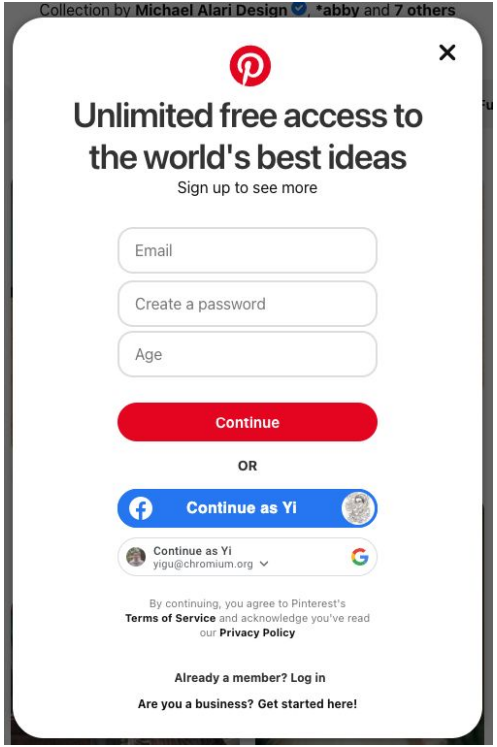



# What's next: Other IdP use cases

- Personalized button
- Early explorations
  - Access tokens
  - Refresh tokens (silent access)
  - DPoP API (proof of possession)
  - Non-email user identification (e.g. phone number)
  - Multiple iframes sharing one login prompt



# Q & A