# FedCM Update

## where we are and where we are going

yigu@chromium.org cbiesinger@chromium.org

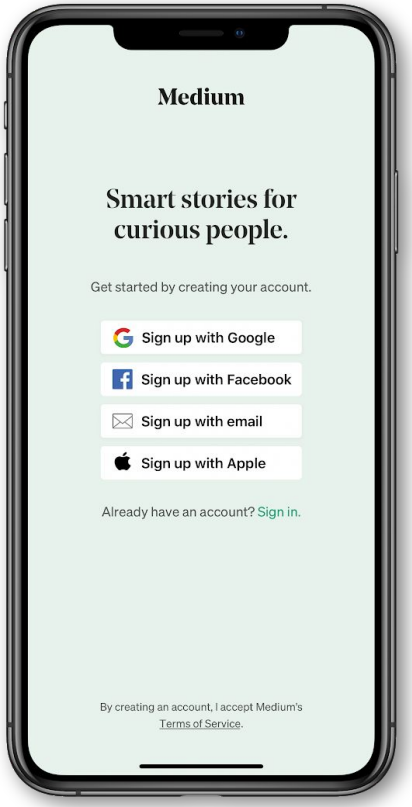
# Why Federated Credentials?

**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

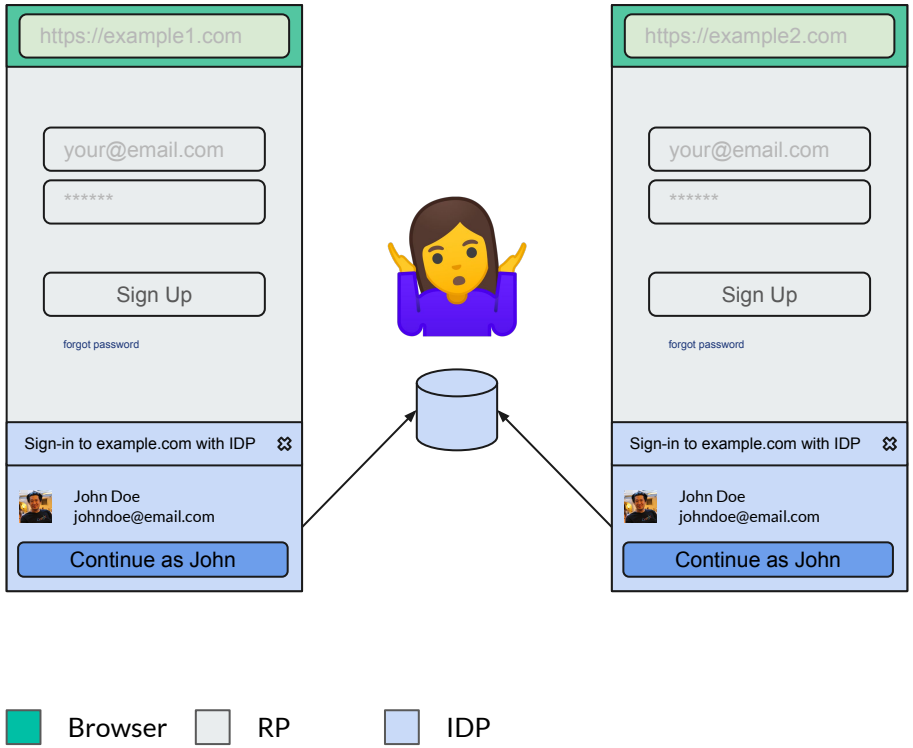
By design, identity federation was built on top of low-level primitives*.

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

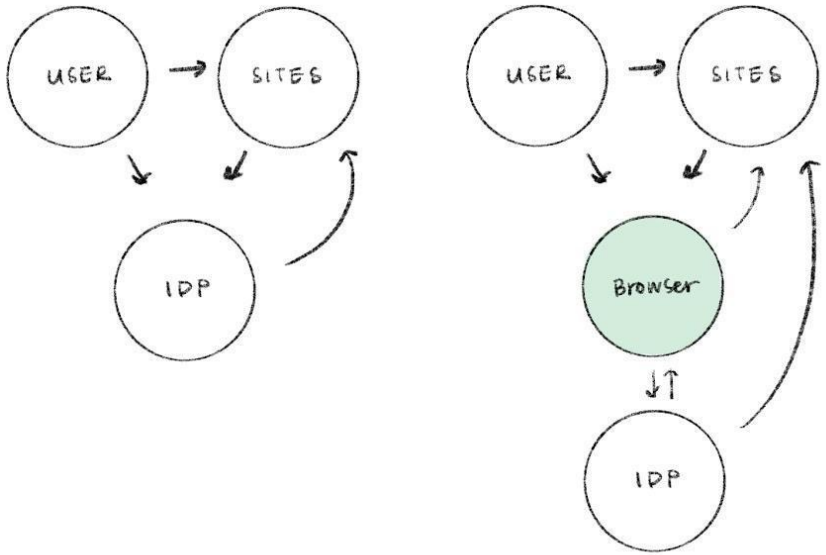
Unfortunately, we can't distinguish tracking from federation.

* iframes, third party cookies, redirects

## The classification Problem



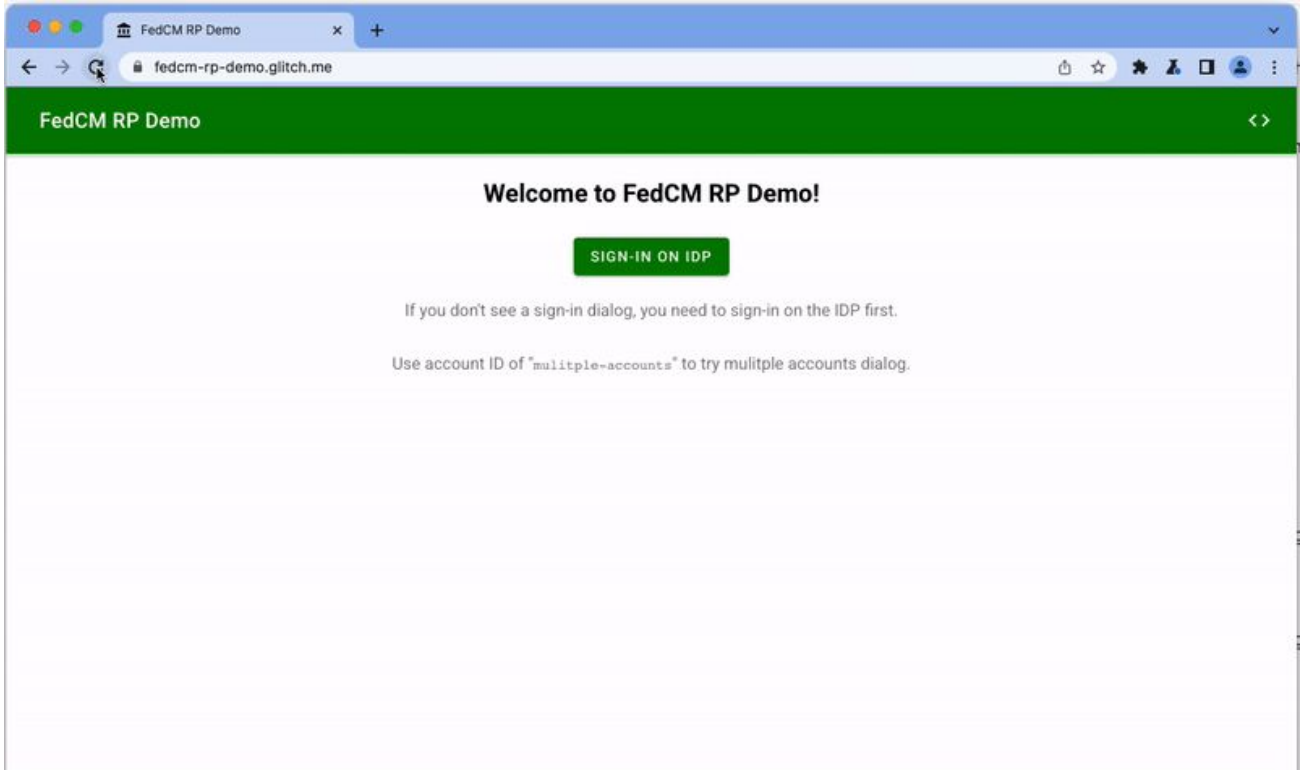
# How?



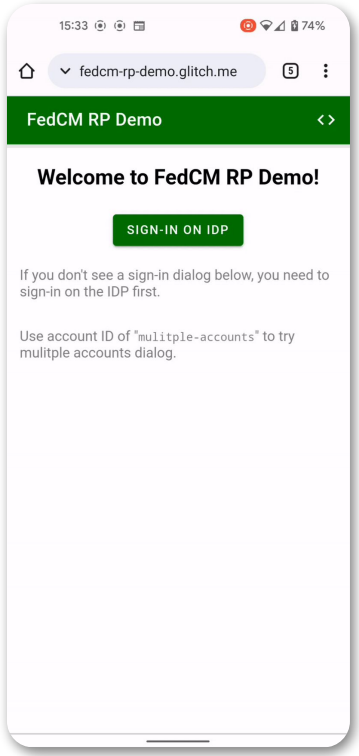
# How?

| 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.

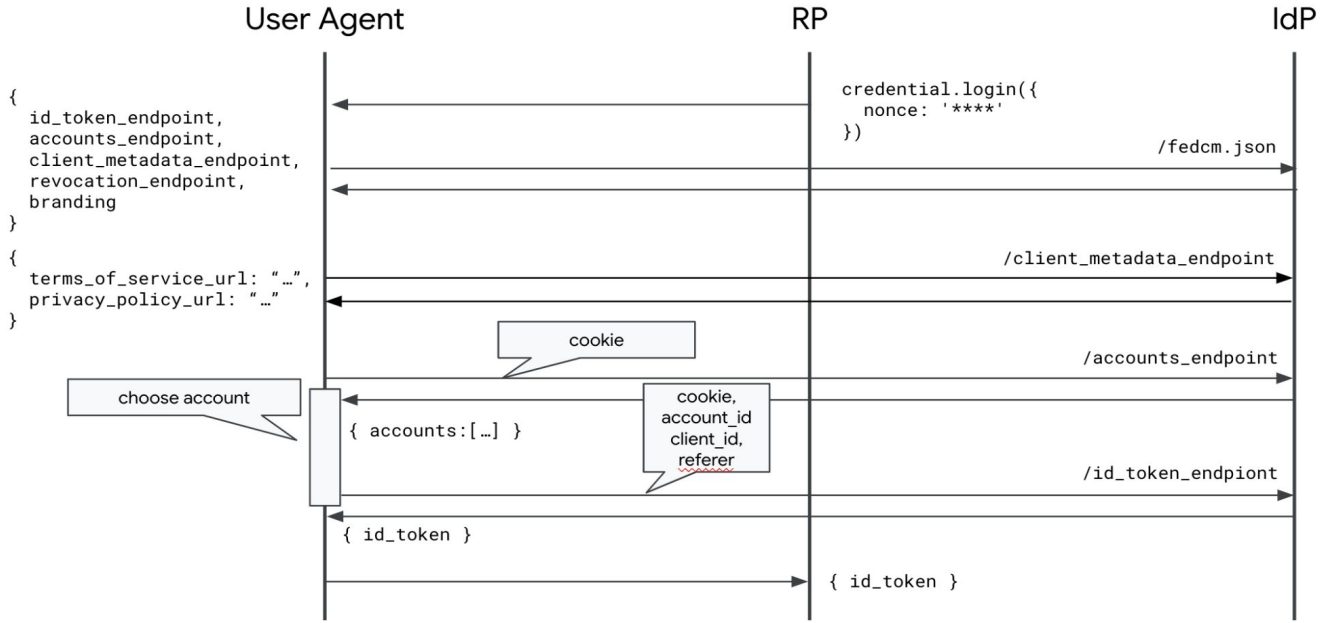
# Demo time!


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

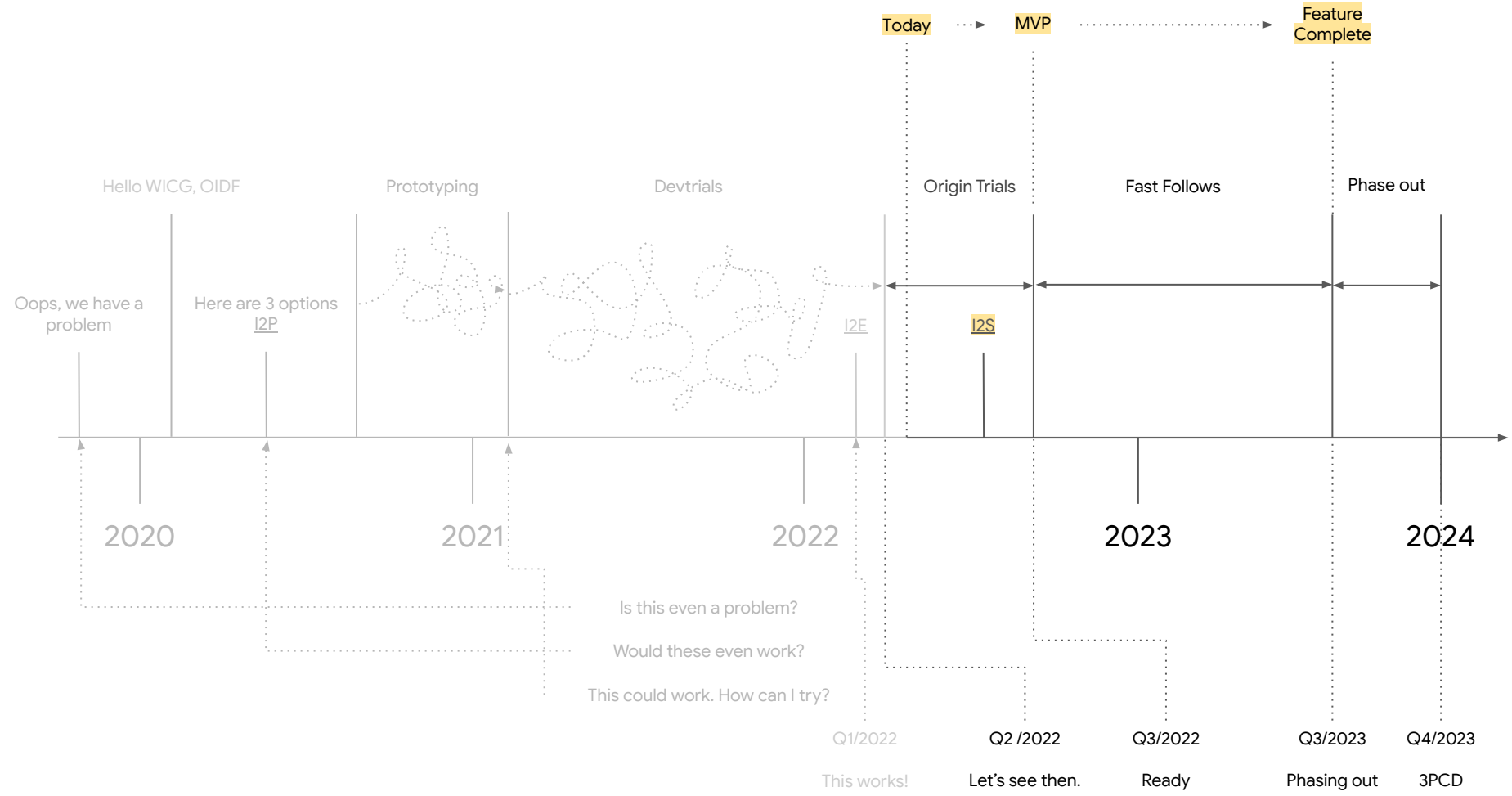
```
var credential = navigator.credentials.get(
    {provider: “https://idp.example/”, client_id: “123”} );
{id_token} = credential.login();



// Also available:

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

# How? The HTTP API




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

# When?

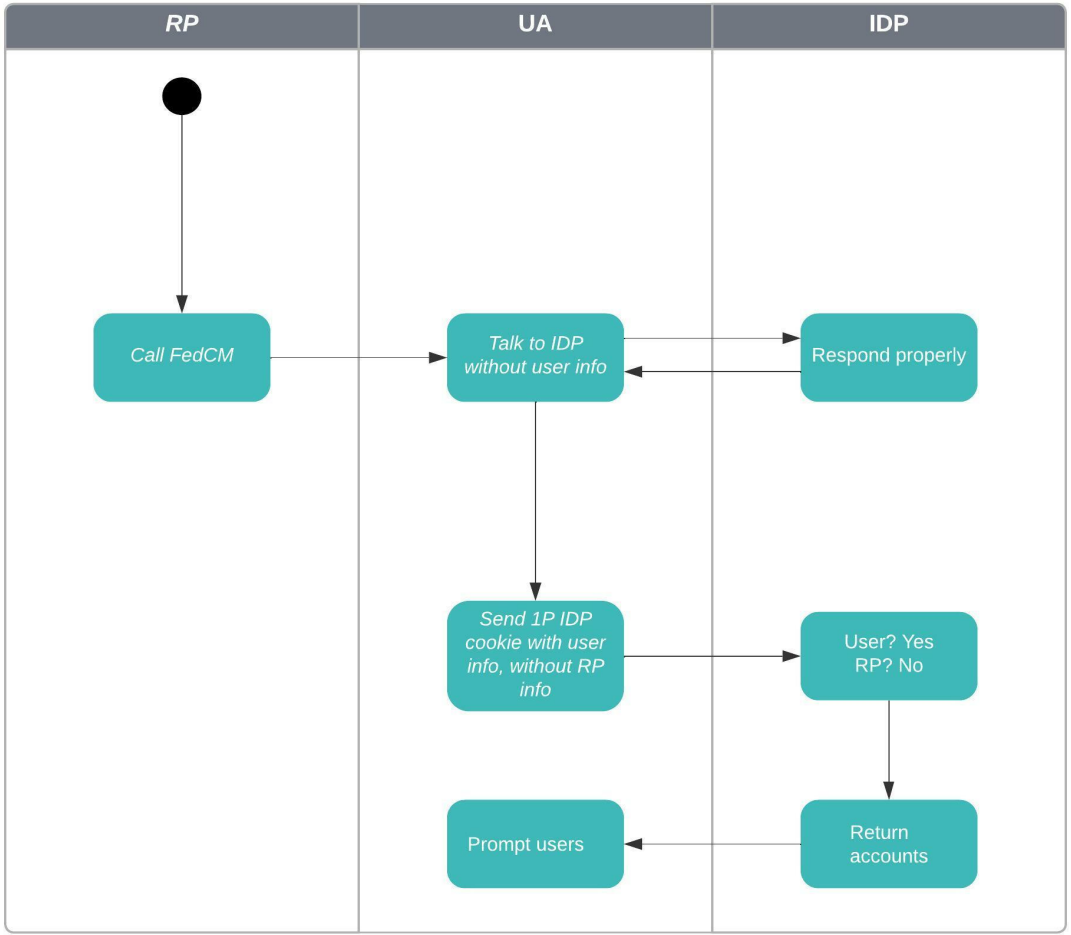

Today
MVP
Feature Complete
Hello WICG, OIDF
Prototyping
Devtrials
Origin Trials
Fast Follows
Phase out
Oops, we have a problem
Here are 3 options
I2P
I2E
I2S
2020
2021
2022
2023
2024
Is this even a problem?
Would these even work?
This could work. How can I try?
Q1/2022
This works!
Q2 /2022
Let's see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

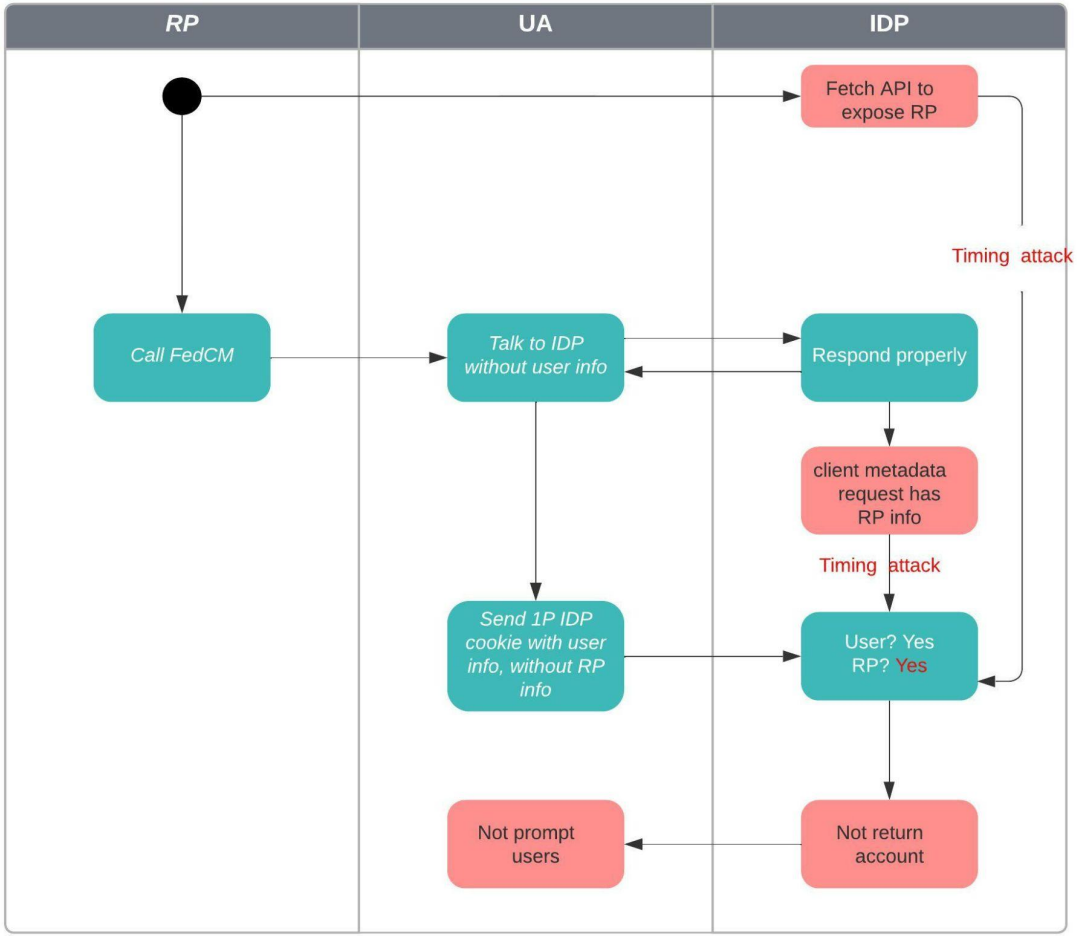
# Community Feedback

- 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, 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


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

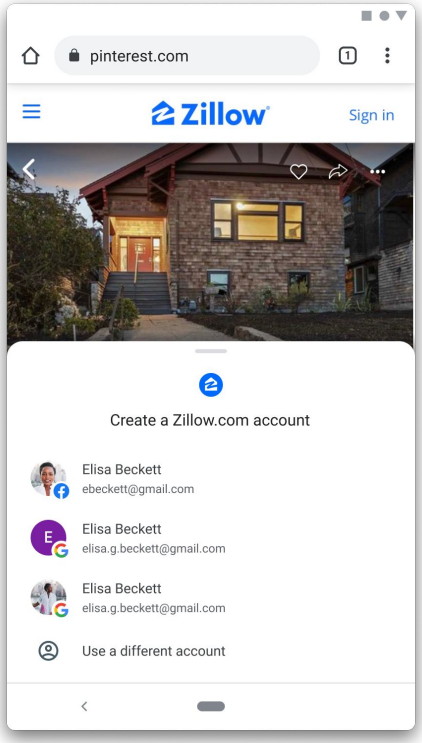

RP
UA
IDP
Fetch API to expose RP
Timing attack
Call FedCM
Talk to IDP without user info
Respond properly
client metadata request has RP info
Timing attack
Send 1P IDP cookie with user info, without RP info
User? Yes
RP? Yes
Not prompt users
Not return account

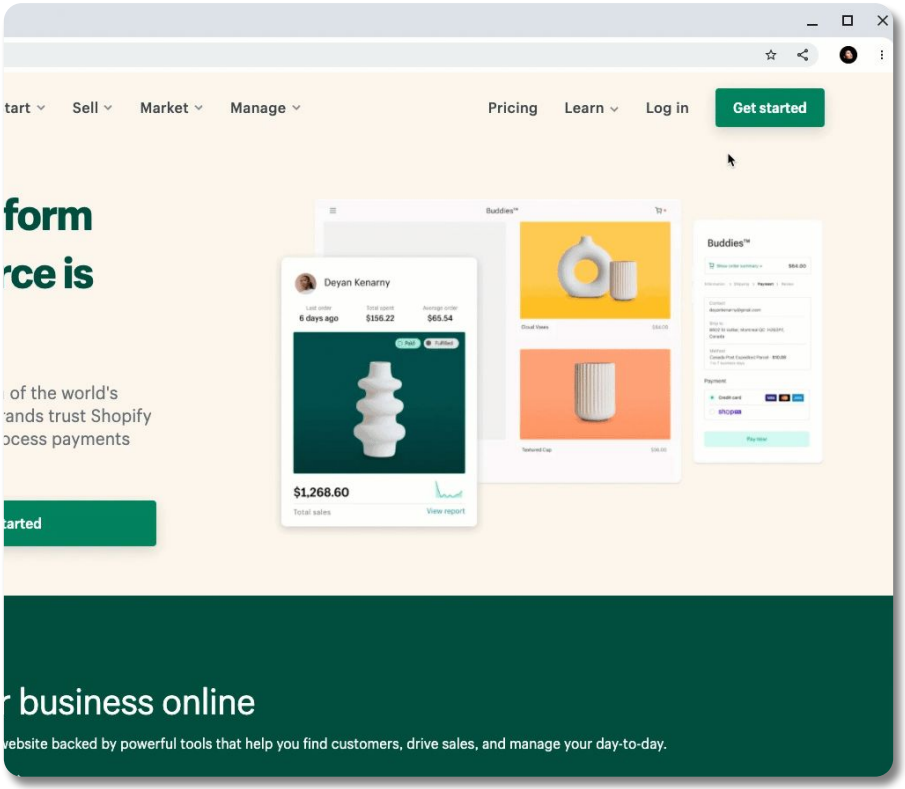
# Options under consideration

- The Push Model
  - IDP push accounts to the browser at the moment of sign-in etc.
  - Solves timing attack, but a bit imposition to IDPs
- The Pull Model with mitigations
  - Always prompt users to at least make tracking observable
    - May depend on a subset of the push model to test “is the user signed in to the IDP”
  - Only pull accounts when necessary
    - Site engagement: users must have interacted with the provider origin in the past
    - Aggregate metrics to penalize suspicious “providers”
      - Click-through rate
      - Invisible UI rate
- Current mental model: pulling accounts when necessary
  - There are fewer browsers than IDPs. We should pull as much responsibility as possible to browsers to offload IDPs (e.g. not have them to pay the price).
  - We want the timing attack to be economically impractical, not mathematically impossible

# What's next: Multiple IDPs?

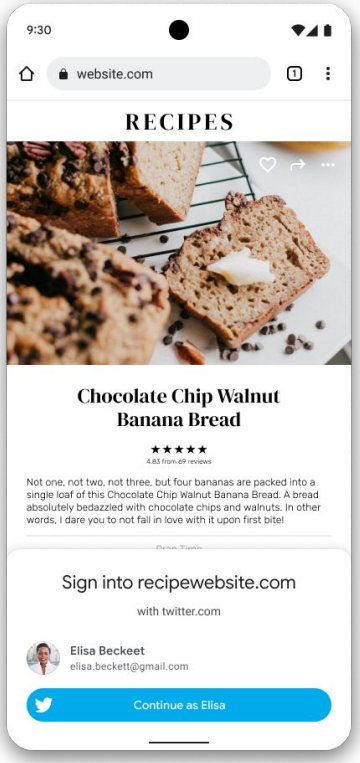
Company logos are illustrative only

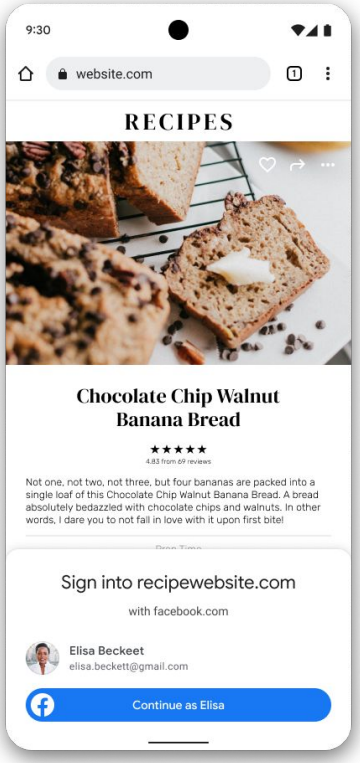


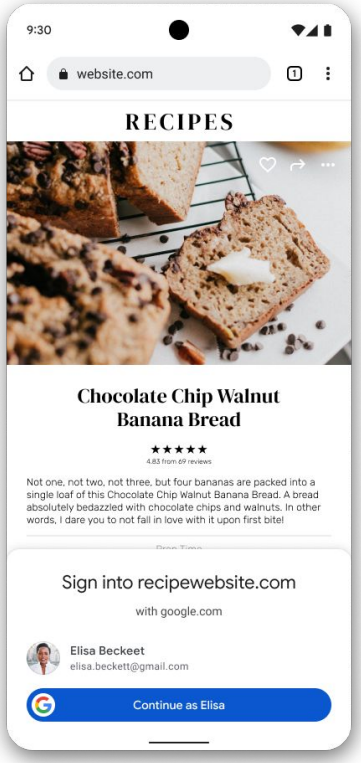



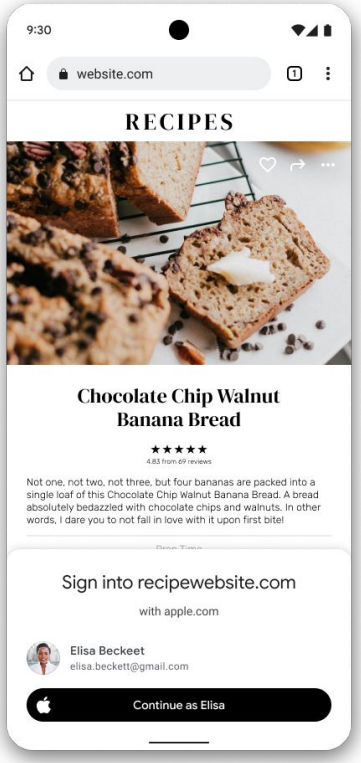
# What's next: Branding?

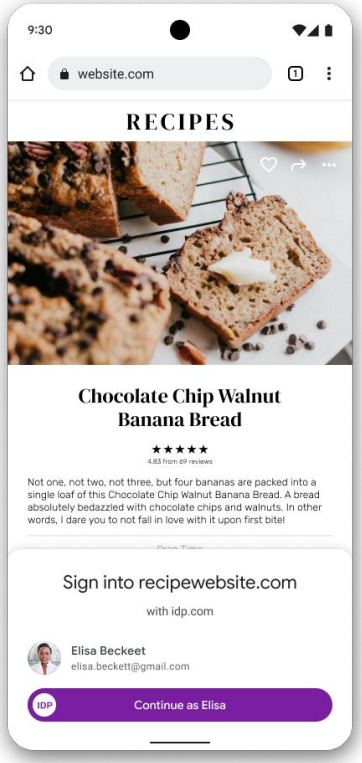
Company logos are illustrative only



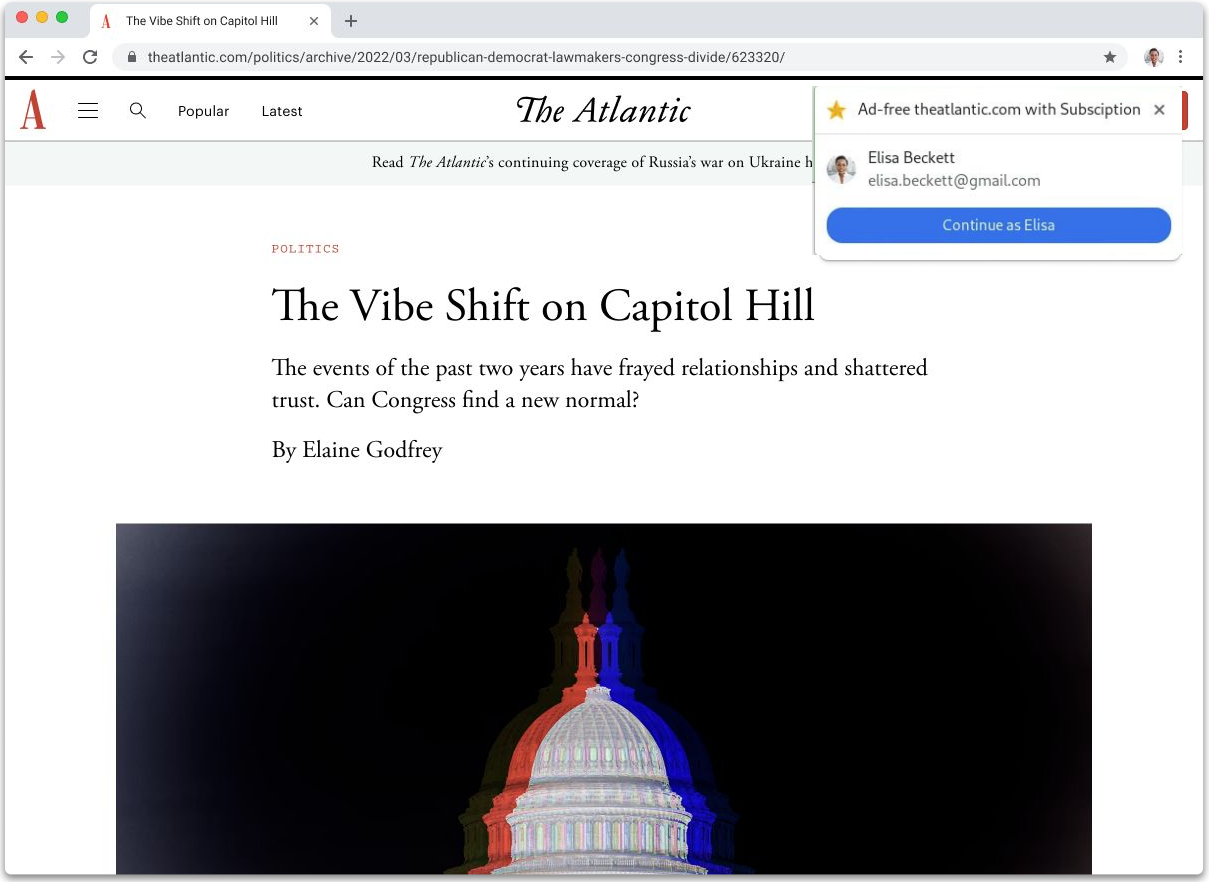



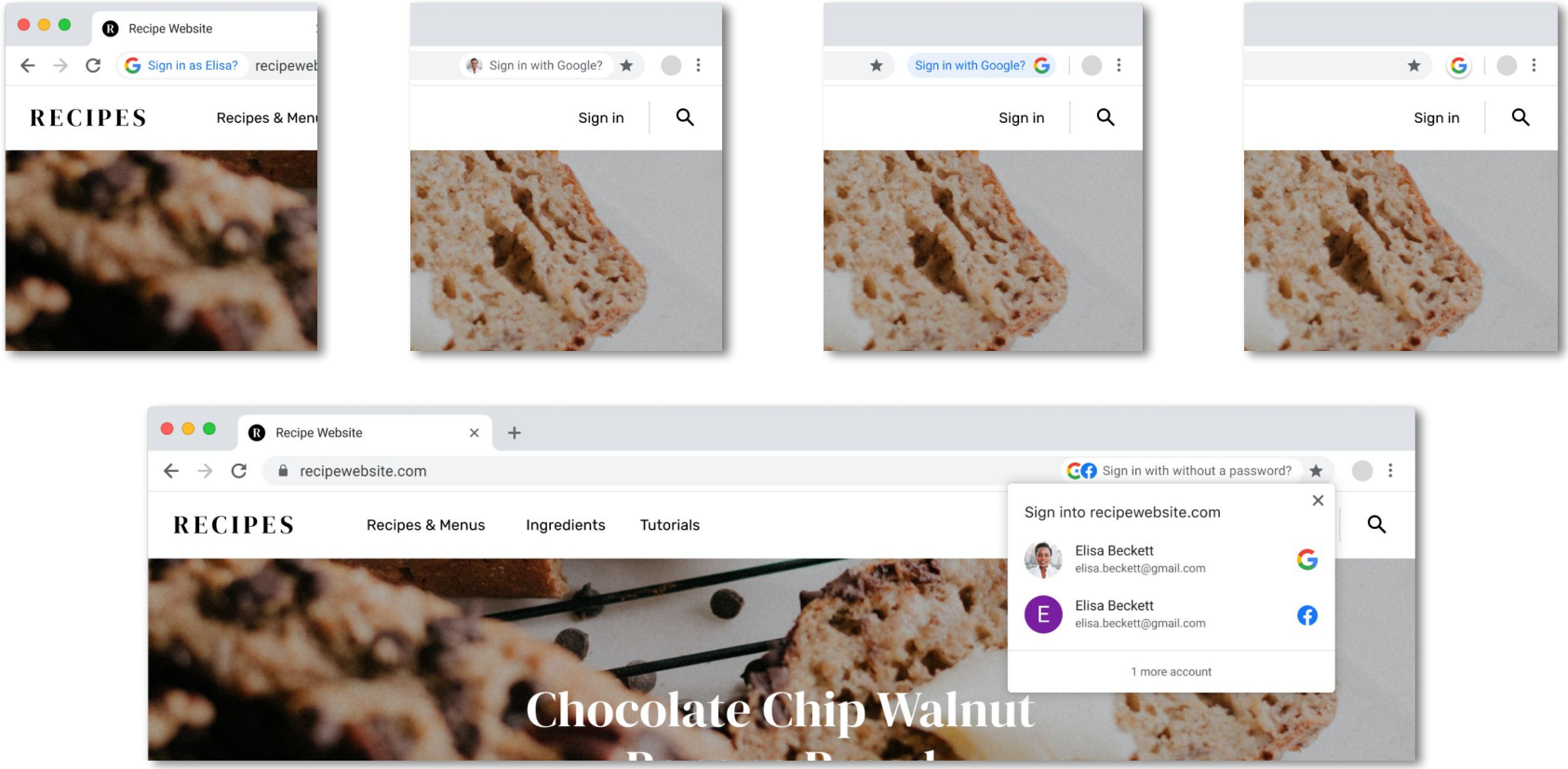
# What's next: Other Use Cases?

Company logos are illustrative only



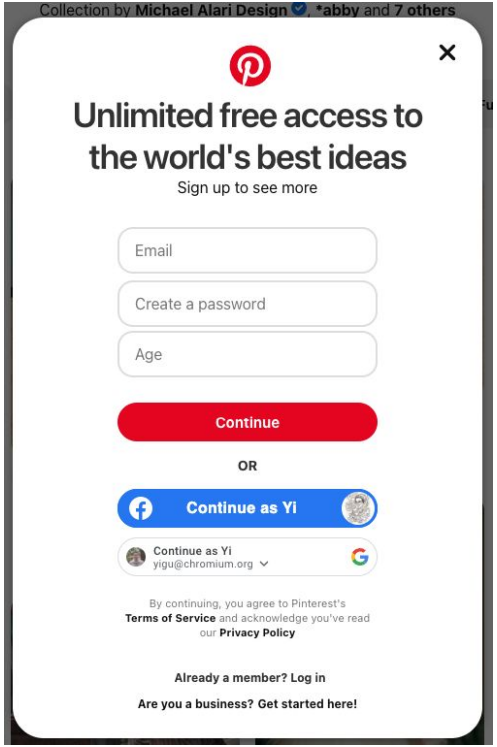
# What's next: previously inaccessible UX opportunities?

Company logos are illustrative only



# What's next: Other IdP use cases

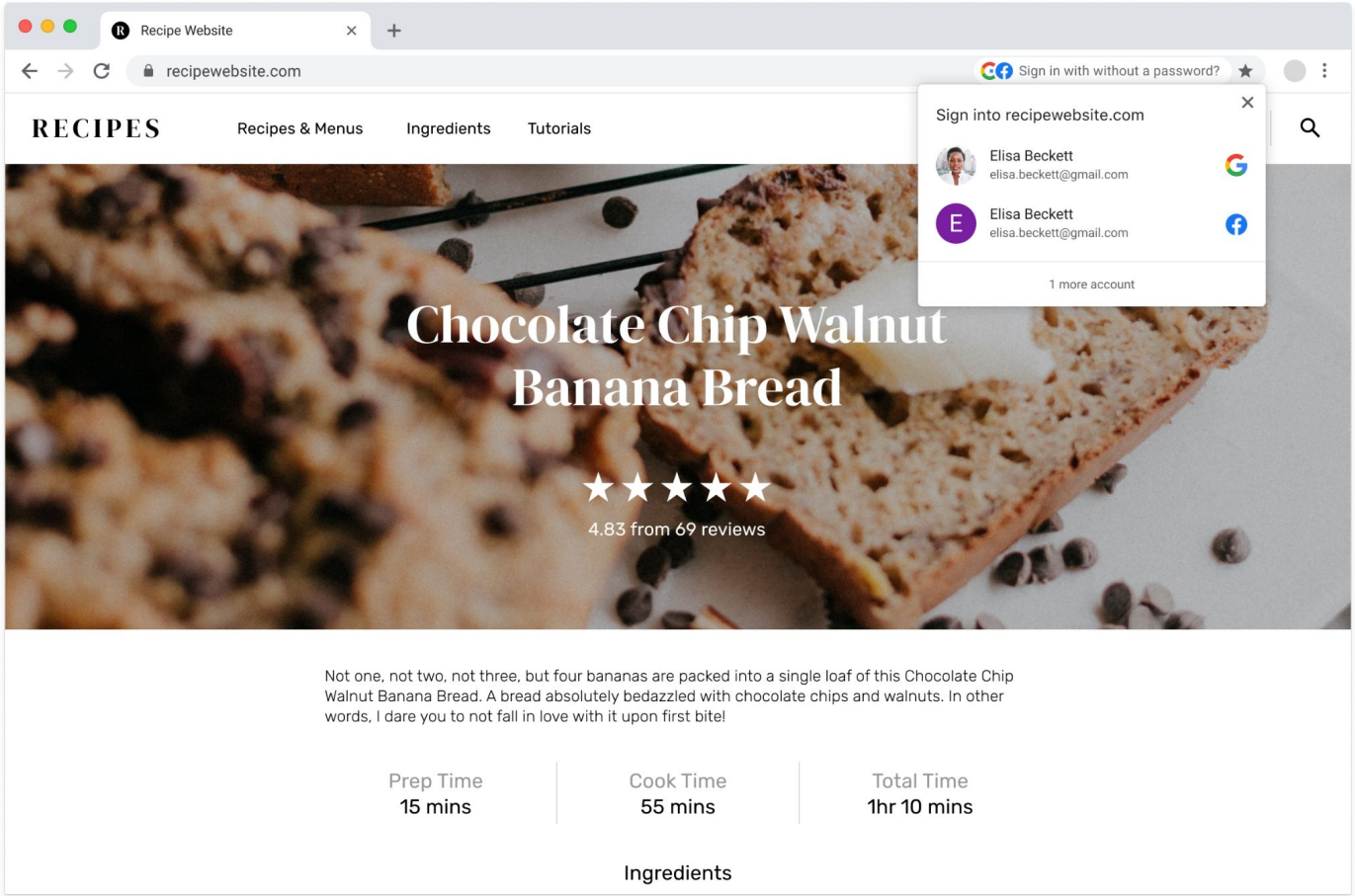
- Personalized button
- Early explorations
  - Access tokens
  - Refresh tokens (silent access)
  - DPoP API (proof of possession)
  - Non-email user identification (e.g. phone number)
  - Multiple iframes sharing one login prompt



# Q & A

ANNEX

# Previously Inaccessible UX



# Why?

## The Pull Model

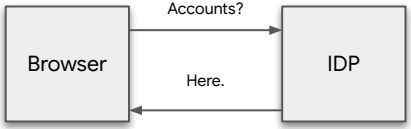
On demand, the browser makes an HTTP request to the IDP that returns the user's accounts.

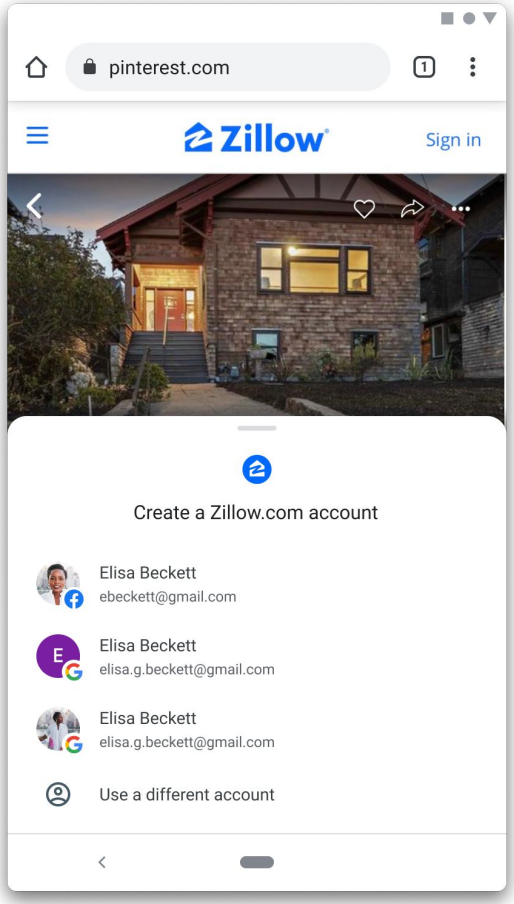
**Pros**

Simple to implement. Always in Sync.

**Cons**

Latency. Timing Attacks.




## The Push Model

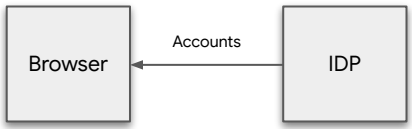
Ahead of time, the IDP saves in the browser the user's accounts.

**Pros**

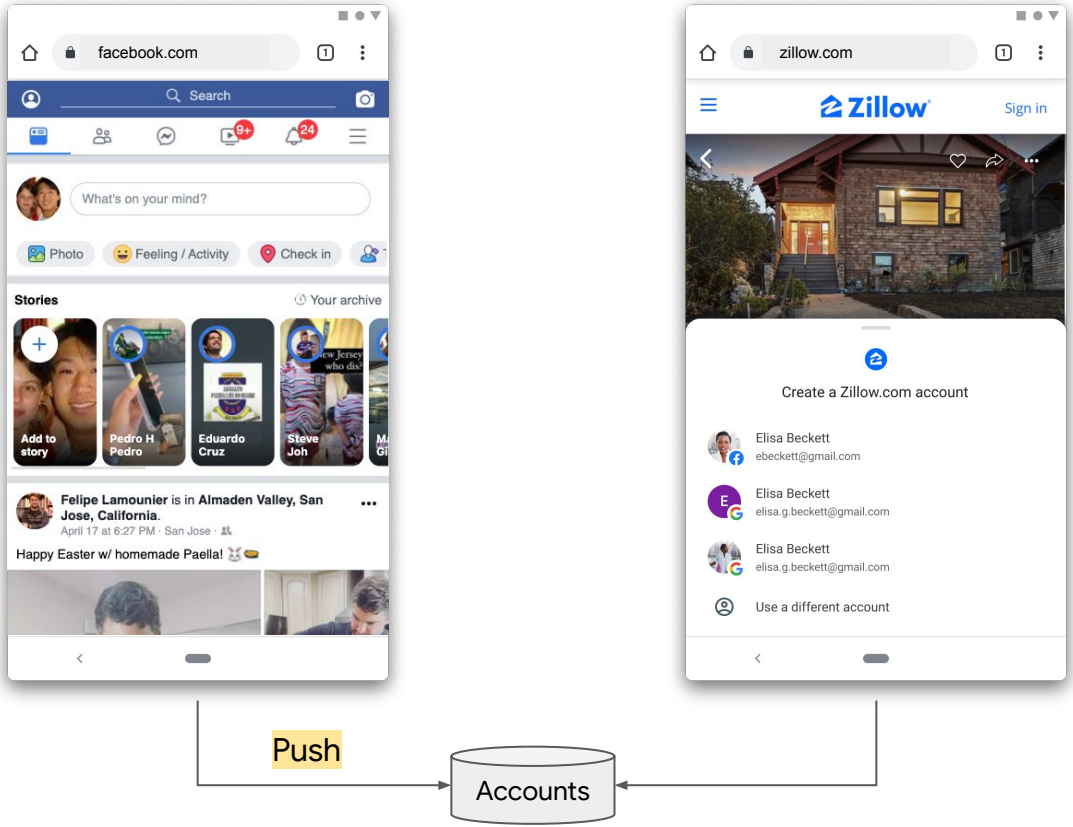
Better UX. No attacks. Allows multiple IDPs.

**Cons**

Can be out of sync, so UI needs to degrade gracefully when it does. IDP announces all accounts rather than only the ones that would use federation.



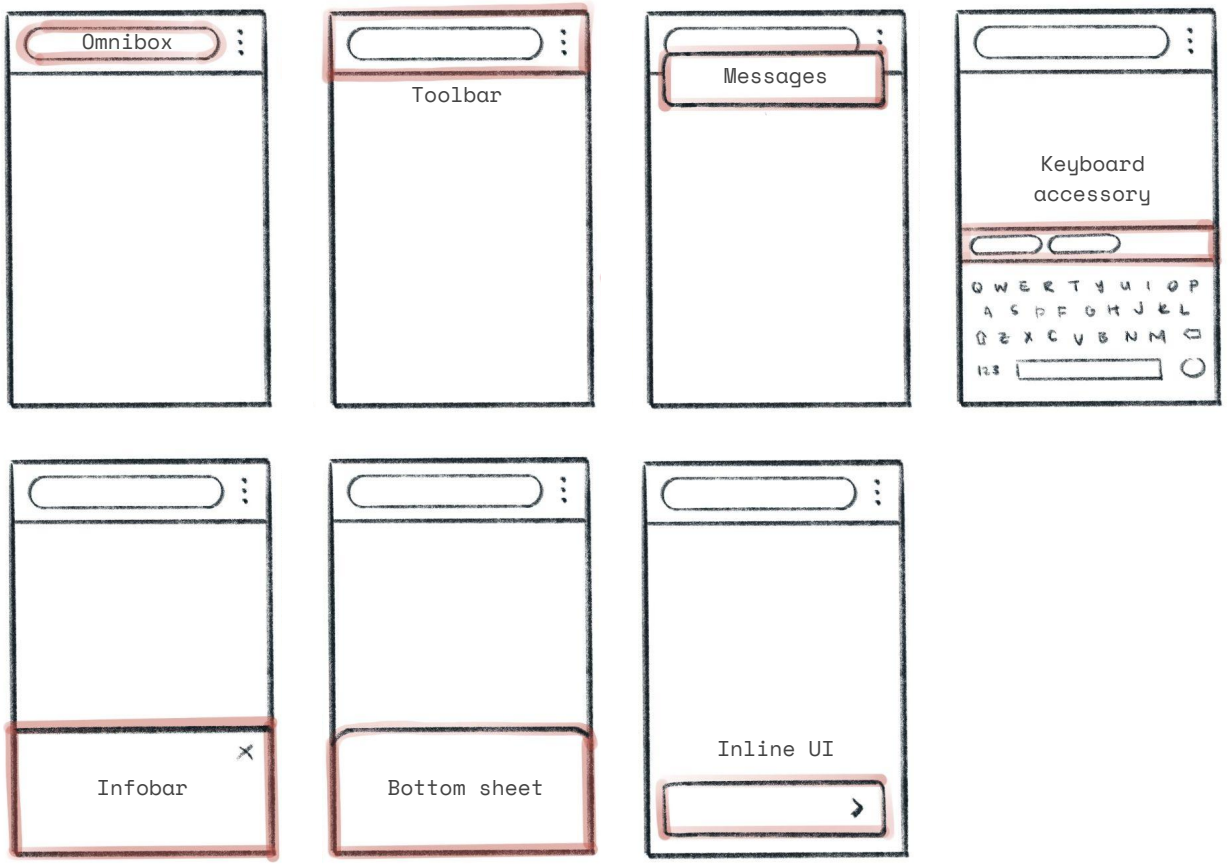
# The Push Model



# Future

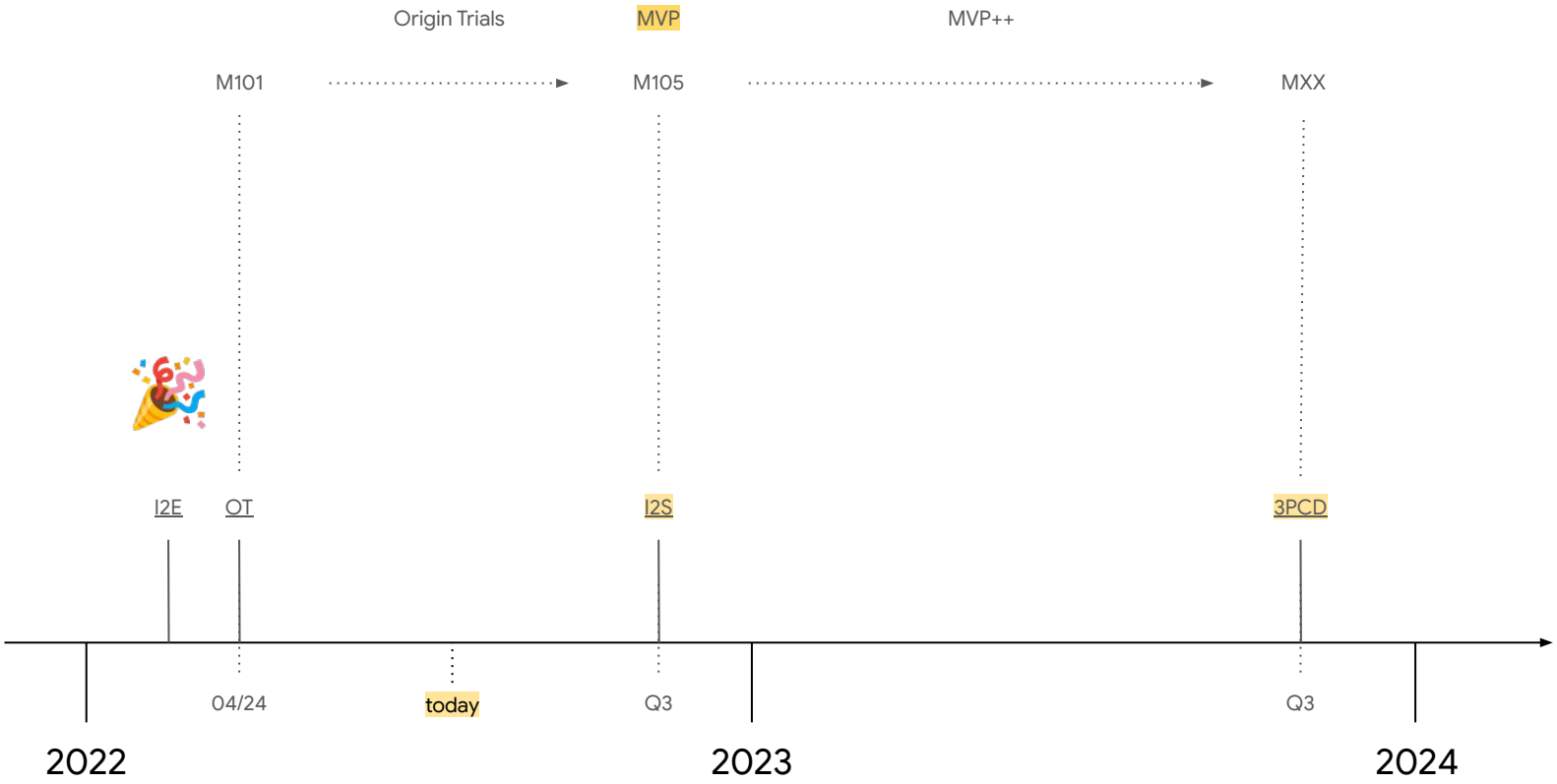
- TODO: add some slides from UX summit

# Possible mobile Chrome surfaces

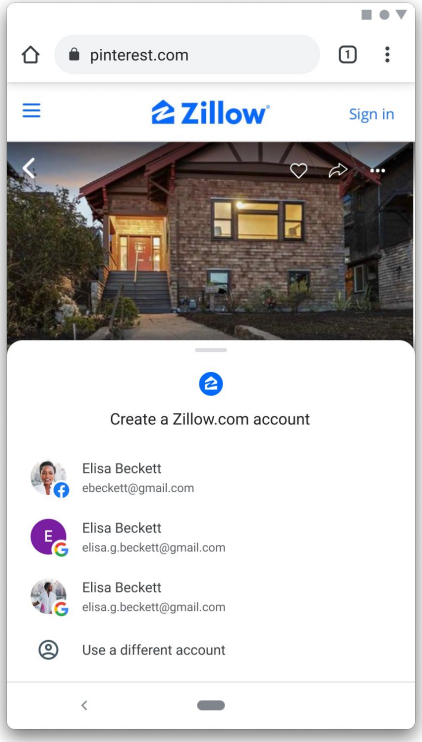


**The last 3 slides (including this one) will be deleted before final submission.**

# Timeline


Origin Trials
MVP
MVP++
M101
M105
MXX
I2E
OT
I2S
3PCD
04/24
today
Q3
Q3
2022
2023
2024

# Multiple IDPs



**Please MAKE A COPY of this document before proceeding.**

# Hopin Resources for Speakers*

**Before your session:**

- Check your network connectivity and browser compatibility
- Sign up for a Hopin demo or contact us at blinkon@chromium.org with questions

**Additional resources:**

- Hopin Knowledge Center
- Quick Troubleshooting Reference Guide
- Sessions Tutorial - During the Event
- Tips for Speaking in and Moderating Sessions
    - Your session is an Open Session (anyone can participate on screen)

** Please note that this slide is for speakers only. Please feel free to delete this slide before sharing.*

# Breakout Session Instructions*

**To join your session:**

- Head to the calendar invite or the Sessions tab in Hopin and find the Session you'll be hosting
- Click Share Audio and Video in the center of the Session screen
    - If you haven't allowed access to your camera or mic in the event, you'll be prompted to do so. Once you see yourself on screen, you're live to your audience.

**To share your screen:**

- Click the Screen sharing icon at the bottom of the page
- Switch to Chrome Tab on the popup window and choose the required browser tab
- Check the Share audio box
- Click Share to start sharing

**Your session will be automatically recorded.**

** Please note that this slide is for speakers only. Please feel free to delete this slide before sharing.*