



FedCM Update

where we are and where we are going

yigu@chromium.org cbiesinger@chromium.org

BlinkOn 16

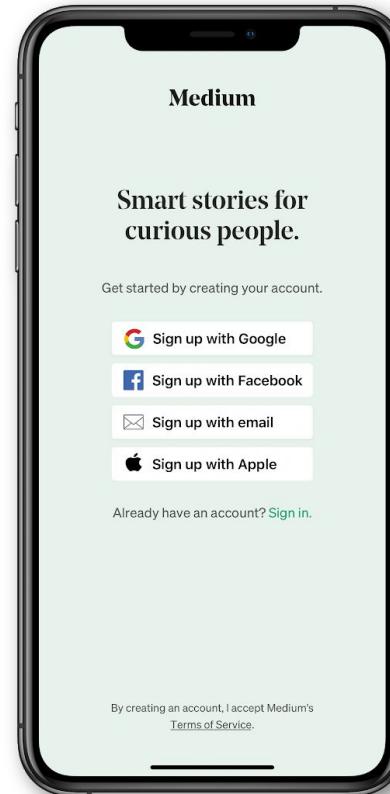
Why Federated Credentials?

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

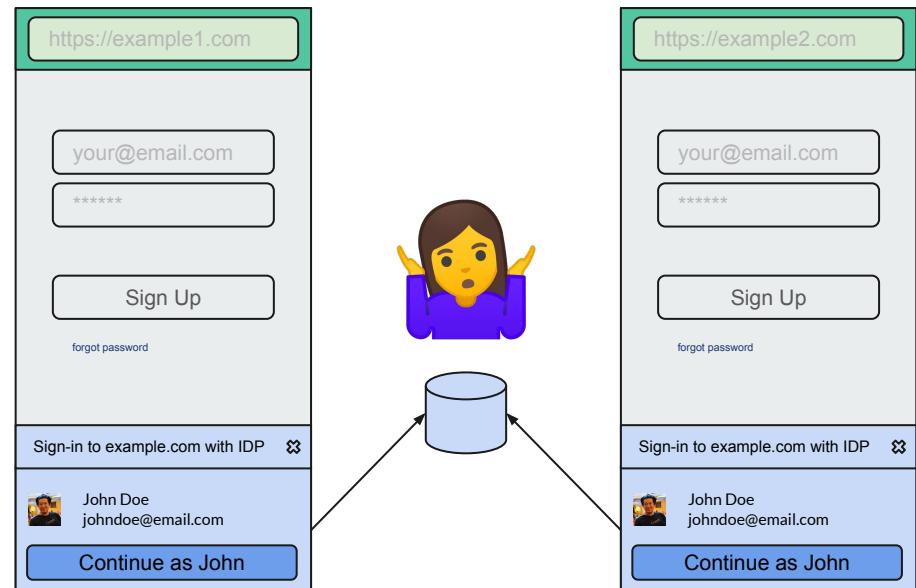
By design, identity federation was built on top of low-level primitives*.

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



Browser

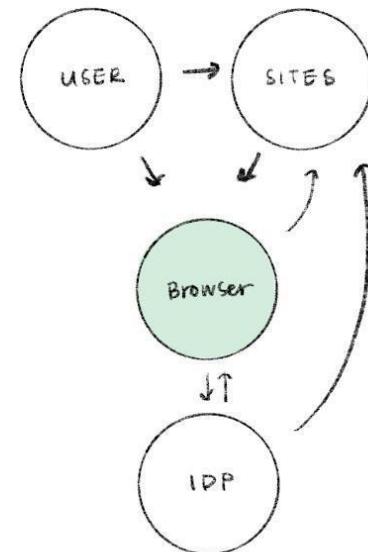
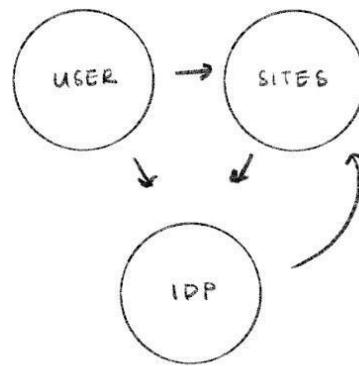


RP



IDP

How?



How?

$O(10s)$

Browsers

Heavy change

$O(100s)$

Identity Providers

Moderate change

$O(M)$

Relying Parties

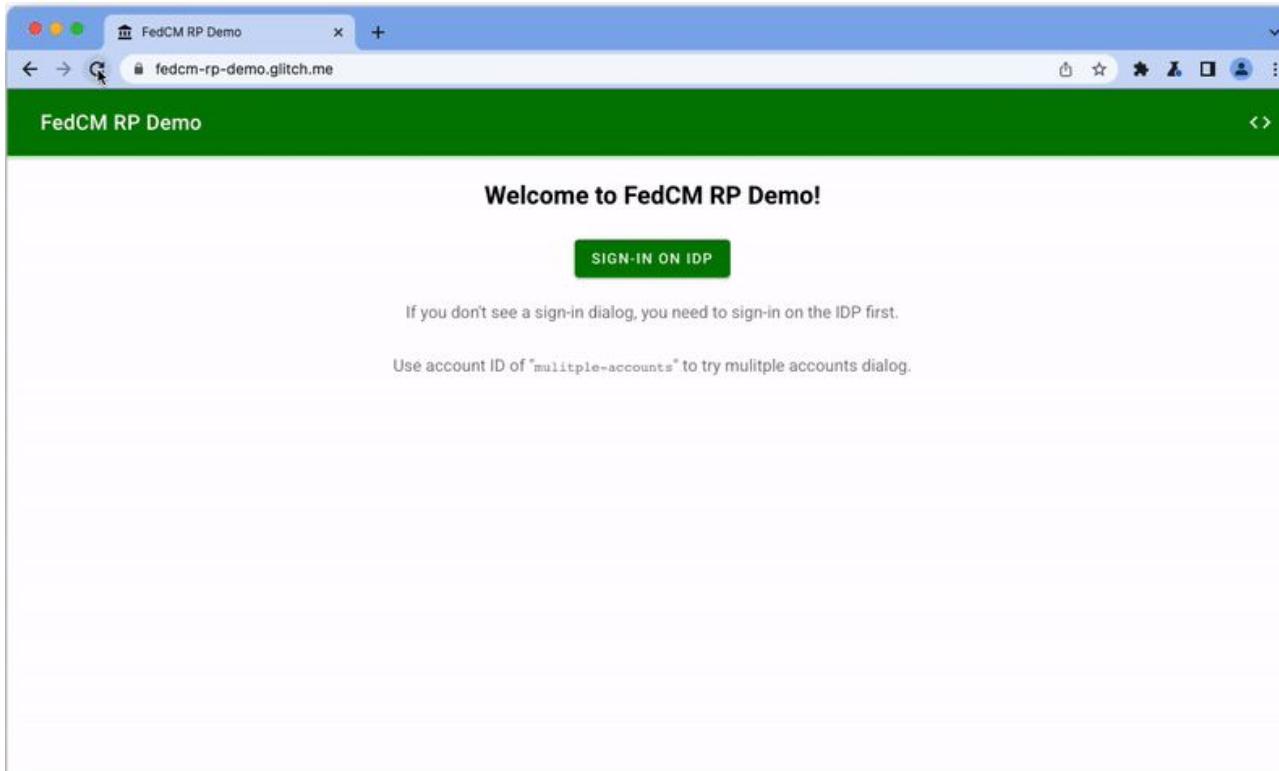
Backwards compatible

$O(B)$

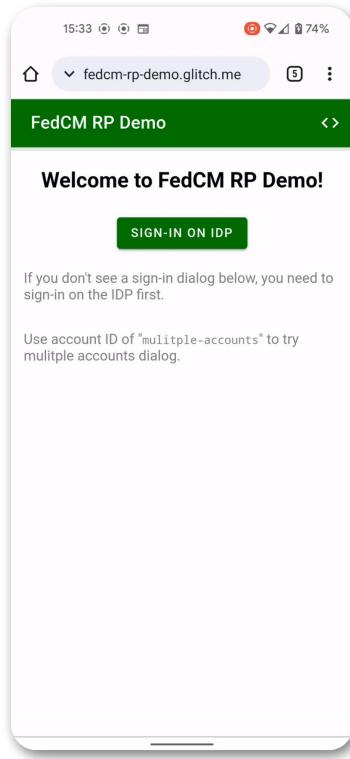
Users

No behavioral changes

Demo time!



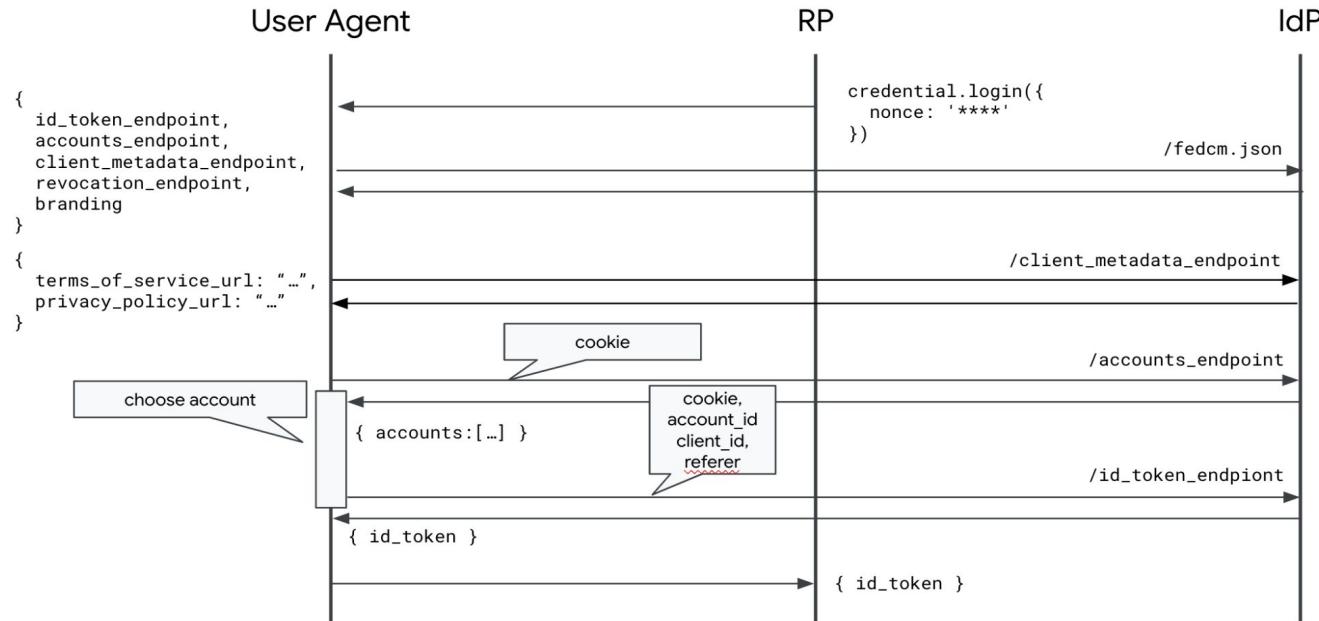
Demo time!



How? The JavaScript API

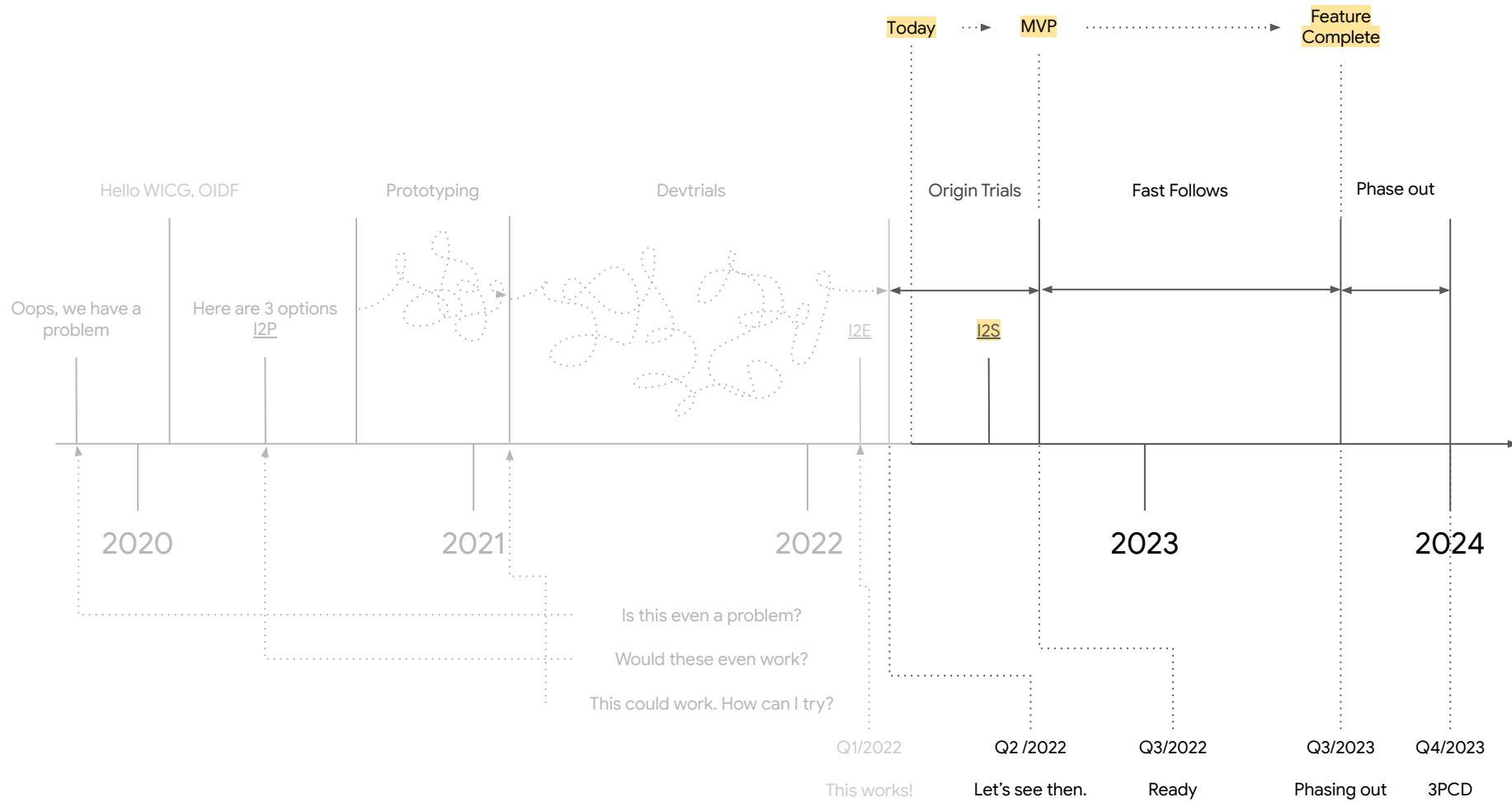
```
var credential = navigator.credentials.get(  
    {provider: "https://idp.example/", client_id: "123"} ) ;  
{id_token} = credential.login();  
  
// Also available:  
  
credential.logout();  
credential.revoke();
```

How? The HTTP API



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

When?

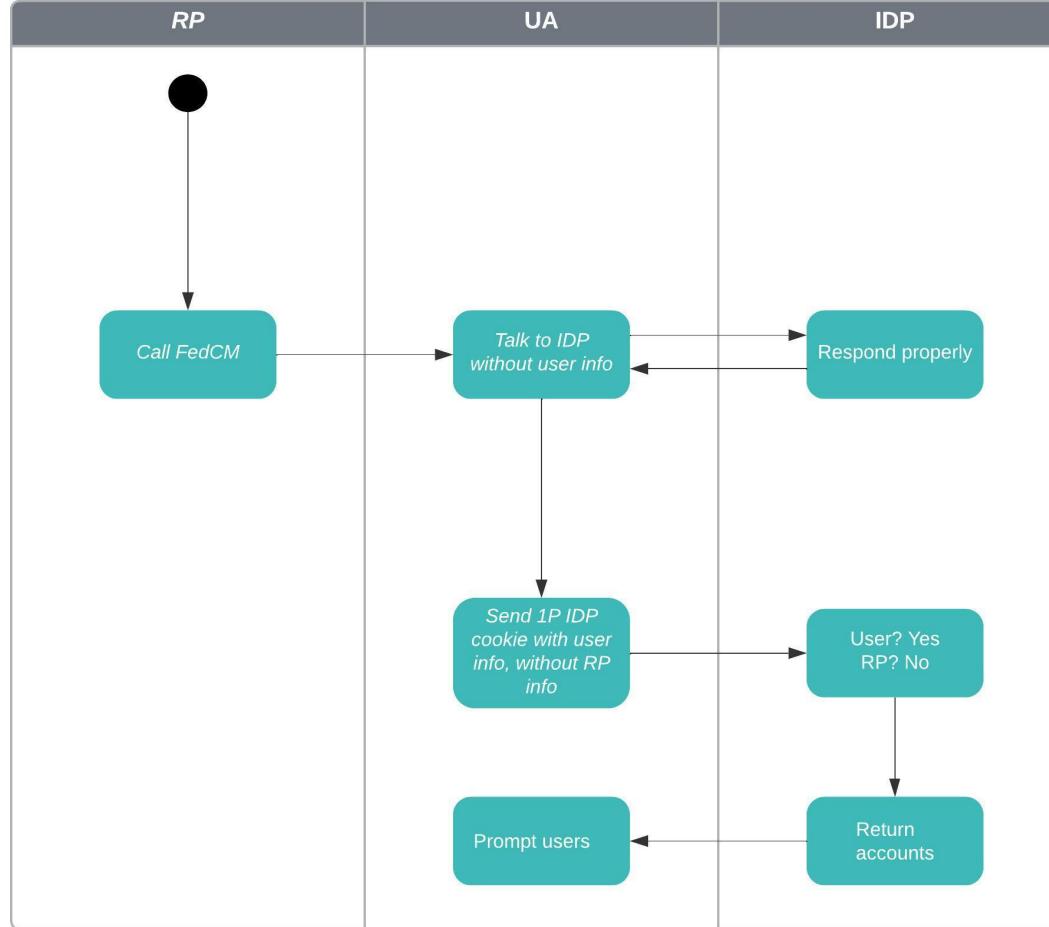


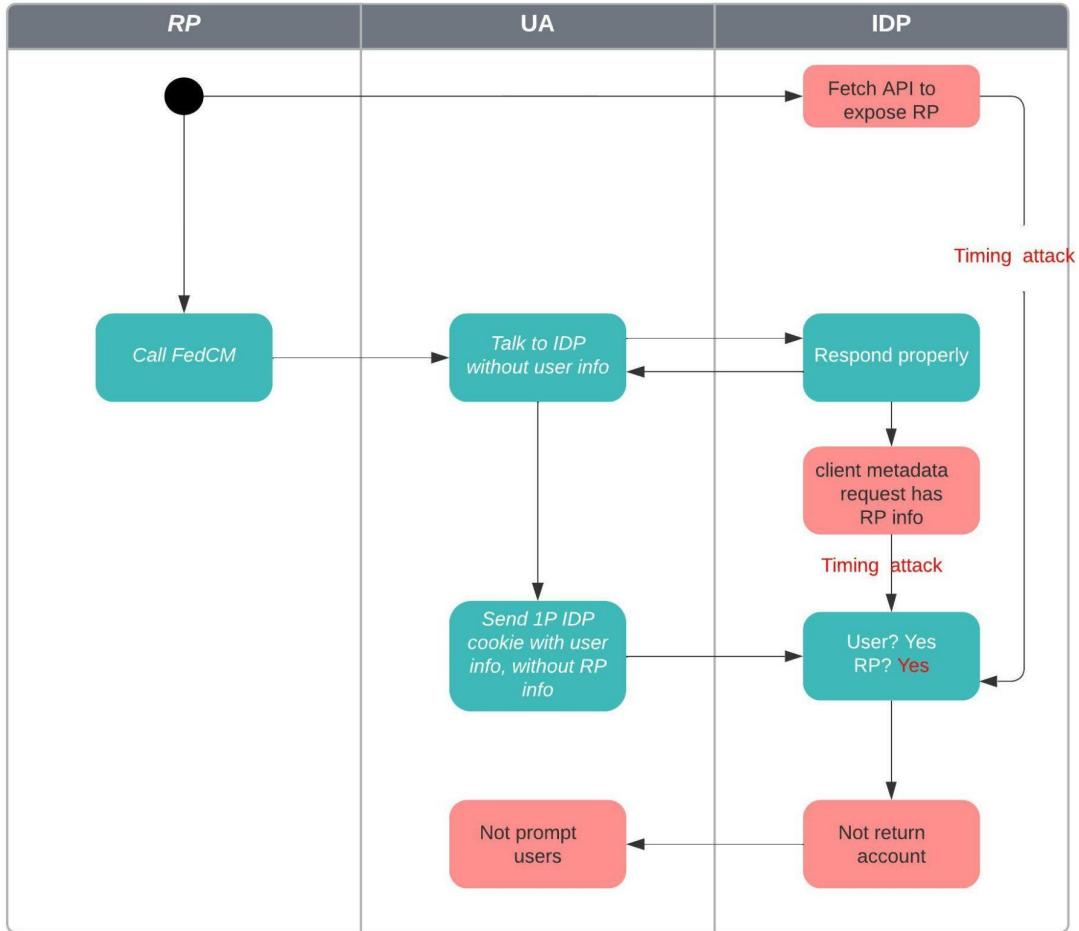
Community Feedback

- [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



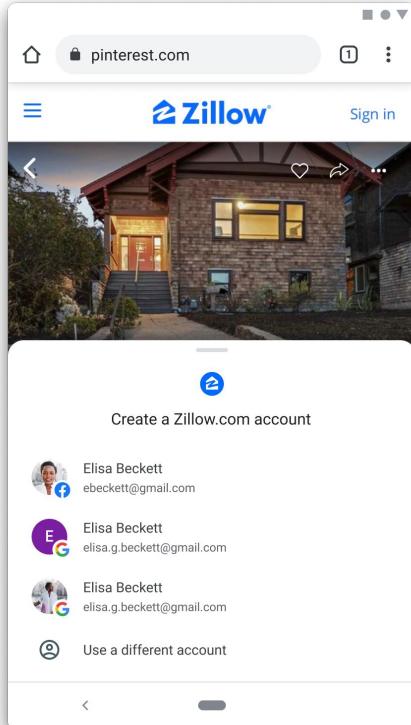


Options under consideration

- 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?

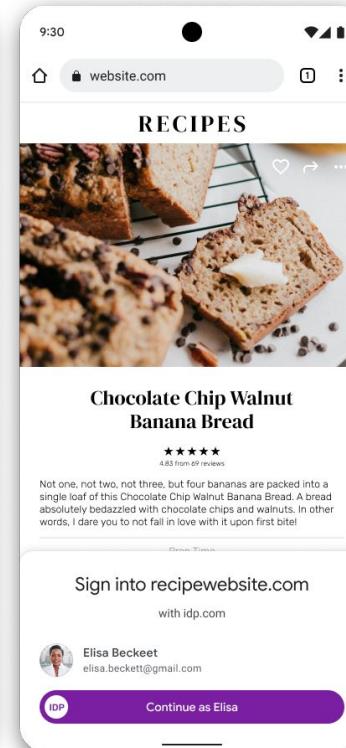
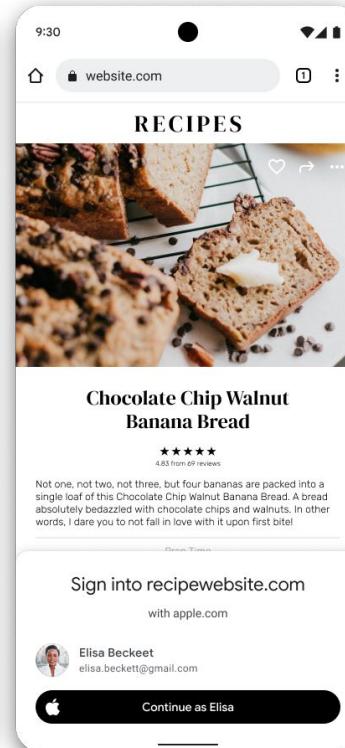
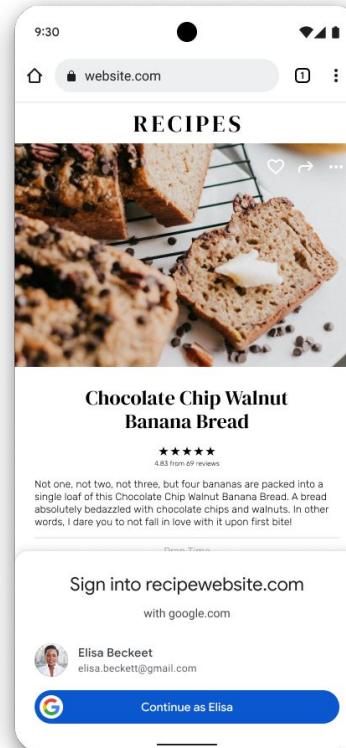
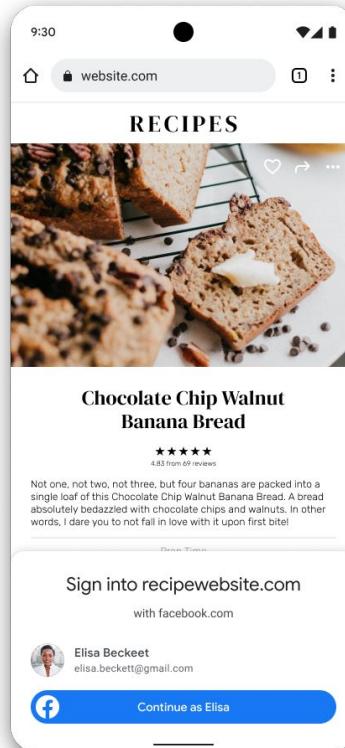
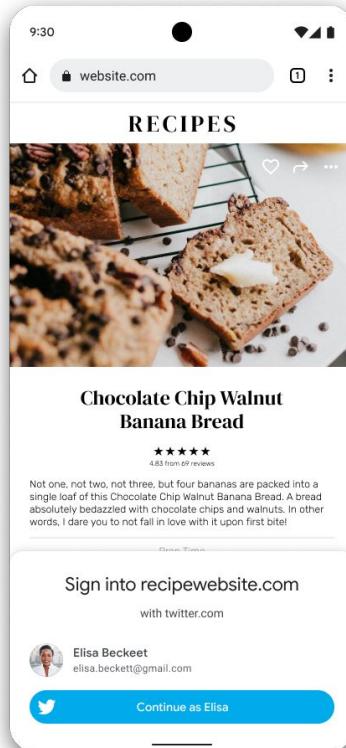
Company logos are illustrative only



A screenshot of the Shopify homepage. At the top, there are navigation links: 'Start', 'Sell', 'Market', 'Manage', 'Pricing', 'Learn', and a 'Log in' button, followed by a 'Get started' button. The main heading reads 'form
orce is'. Below this, there is a section about Shopify's payment processing: 'of the world's brands trust Shopify to process payments'. To the right, there are two examples of Shopify stores: 'Buddies™' and 'Deyan Kenarny'. The 'Buddies™' store shows a product page for a white vase, with metrics: 'Last order 6 days ago', 'First order \$156.22', 'Average order \$65.54', 'Total sales \$1,268.60', and a 'View report' button. The 'Deyan Kenarny' store shows a product page for a white vase, with metrics: 'Last order 6 days ago', 'First order \$156.22', 'Average order \$65.54', 'Total sales \$1,268.60', and a 'View report' button. At the bottom, there is a large green button with the text 'Start your business online'.

What's next: Branding?

Company logos are illustrative only

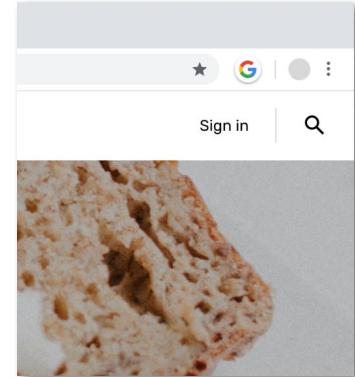
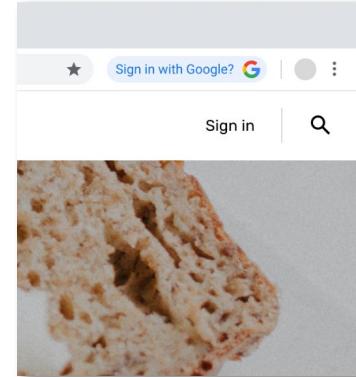
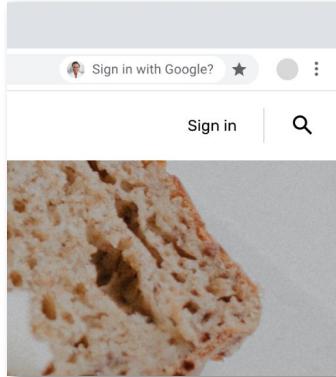
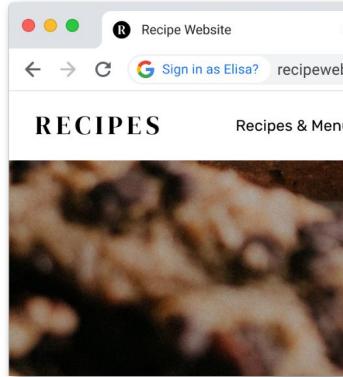


The screenshot shows a web browser window displaying an article from The Atlantic titled "The Vibe Shift on Capitol Hill". The article is categorized under "POLITICS" and is written by Elaine Godfrey. The main image for the article is a dark photograph of the US Capitol dome, with its red, white, and blue colors partially visible.

A user login overlay is visible on the right side of the screen. It features a profile picture of a woman named Elisa Beckett and her email address, elisa.beckett@gmail.com. A blue button labeled "Continue as Elisa" is present. The URL in the browser's address bar is theatlantic.com/politics/archive/2022/03/republican-democrat-lawmakers-congress-divide/623320/.

What's next: previously inaccessible UX opportunities?

Company logos are illustrative only

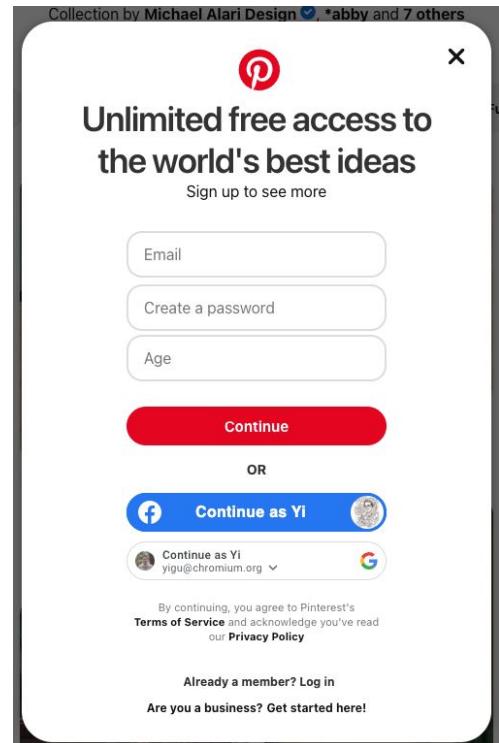
A screenshot of a web browser window for "recipewebsite.com". The main content area shows a close-up image of a light-colored chocolate chip cookie. A sign-in overlay is displayed in the upper right corner, titled "Sign in with without a password?". It contains a "Sign into recipewebsite.com" button, a list of accounts, and social media icons for Google+ and Facebook. The account "Elisa Beckett" is listed twice, each with the email "elisa.beckett@gmail.com".

RECIPES Recipes & Menus Ingredients Tutorials

Chocolate Chip Walnut

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

A screenshot of a web browser displaying a recipe website. The page features a large image of chocolate chip walnut banana bread. Overlaid on the image is the title "Chocolate Chip Walnut Banana Bread" in a large, serif font. Below the title is a five-star rating icon followed by the text "4.83 from 69 reviews". At the top of the page, there is a navigation bar with links for "RECIPES", "Recipes & Menus", "Ingredients", and "Tutorials". A search bar is located in the top right corner. A sign-in modal is open, prompting the user to "Sign into recipewebsite.com". It includes fields for email and password, and social media sign-in options for Google and Facebook. The modal also shows that there is "1 more account".

RECIPES Recipes & Menus Ingredients Tutorials

Sign into recipewebsite.com

Elisa Beckett
elisa.beckett@gmail.com

Elisa Beckett
elisa.beckett@gmail.com

1 more account

Chocolate Chip Walnut Banana Bread

★★★★★

4.83 from 69 reviews

Not one, not two, not three, but four bananas are packed into a single loaf of this Chocolate Chip Walnut Banana Bread. A bread absolutely bedazzled with chocolate chips and walnuts. In other words, I dare you to not fall in love with it upon first bite!

Prep Time
15 mins

Cook Time
55 mins

Total Time
1hr 10 mins

Ingredients

Why?

The Pull Model

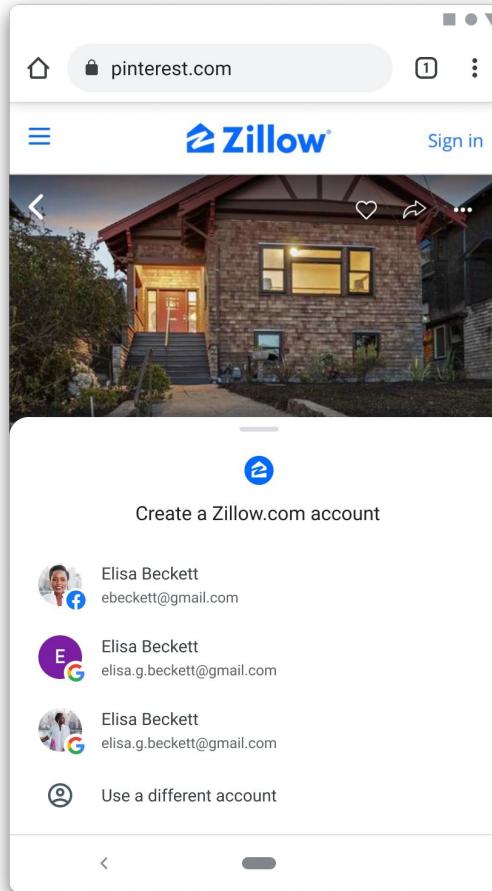
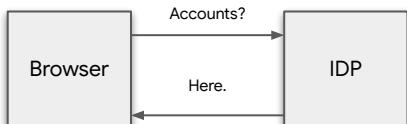
On demand, the browser makes an HTTP request to the IDP that returns the user's accounts.

Pros

Simple to implement. Always in Sync.

Cons

Latency. **Timing Attacks.**



The Push Model

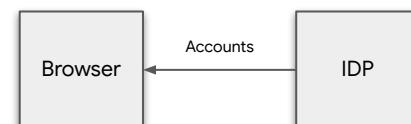
Ahead of time, the IDP saves in the browser the user's accounts.

Pros

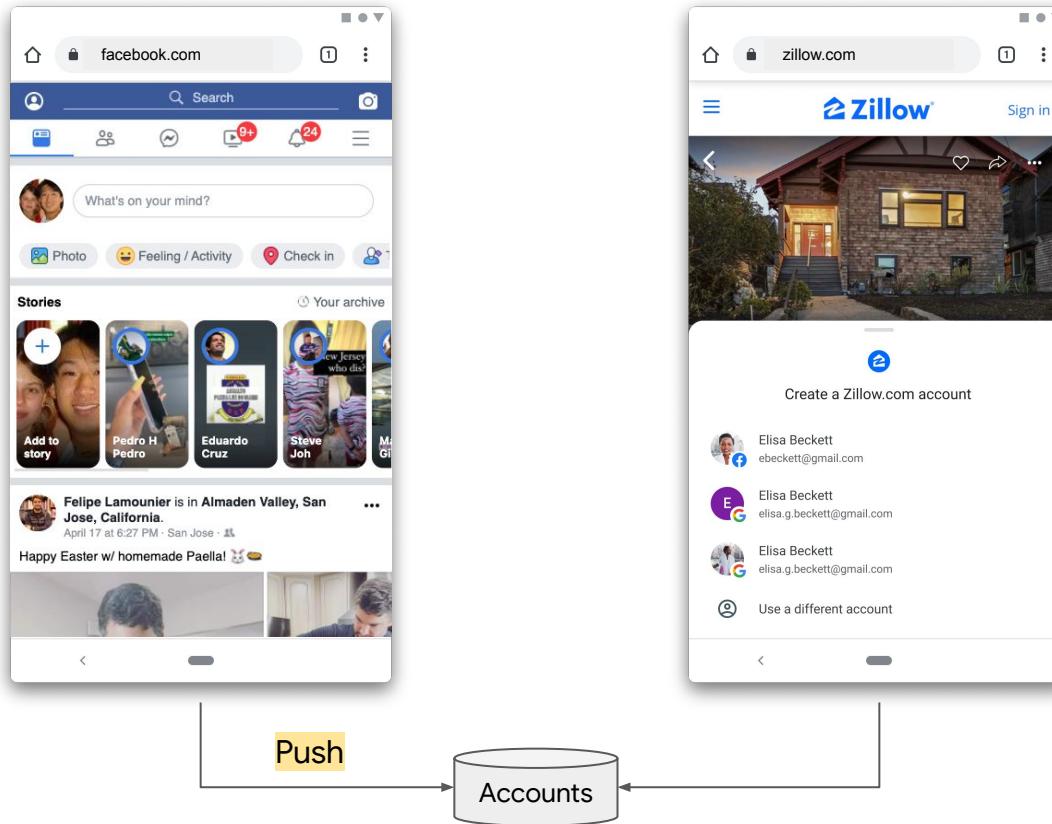
Better UX. No attacks. Allows multiple IDPs.

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.



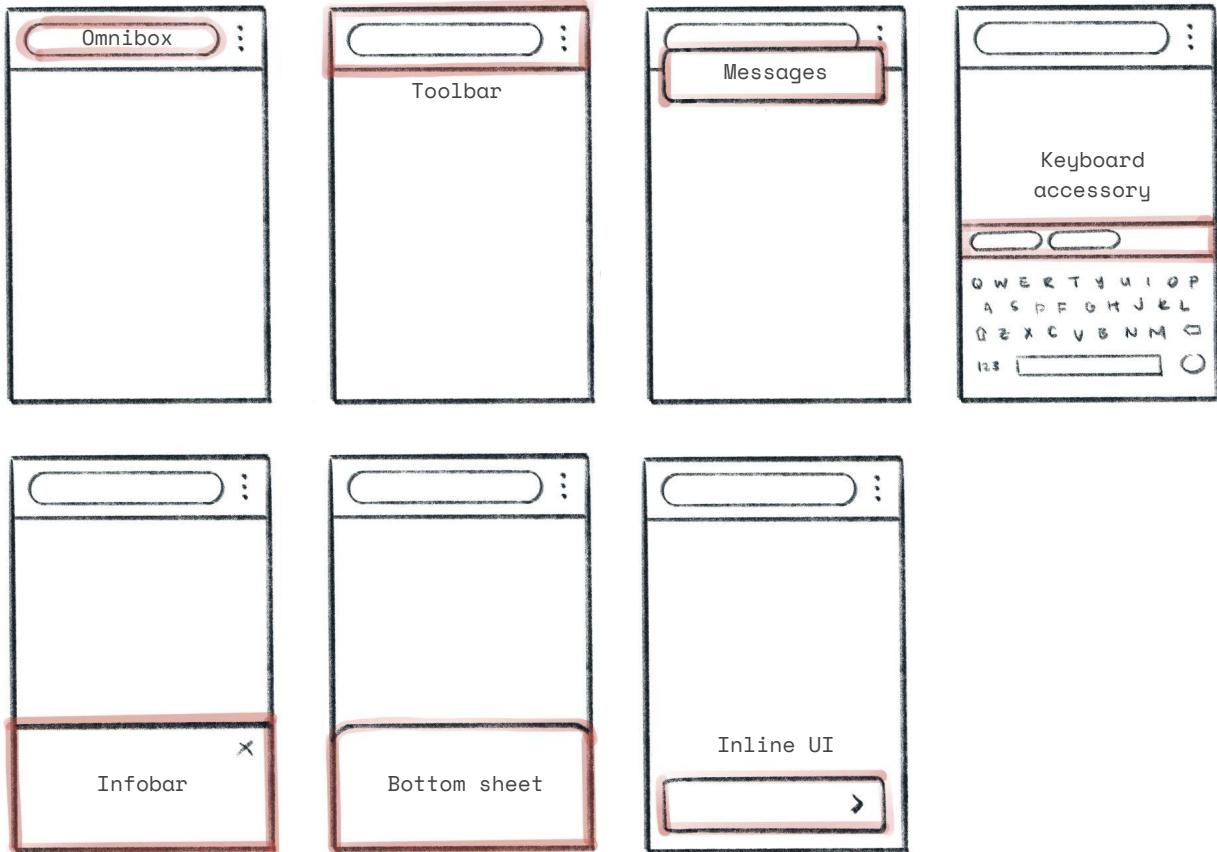
The Push Model



Future

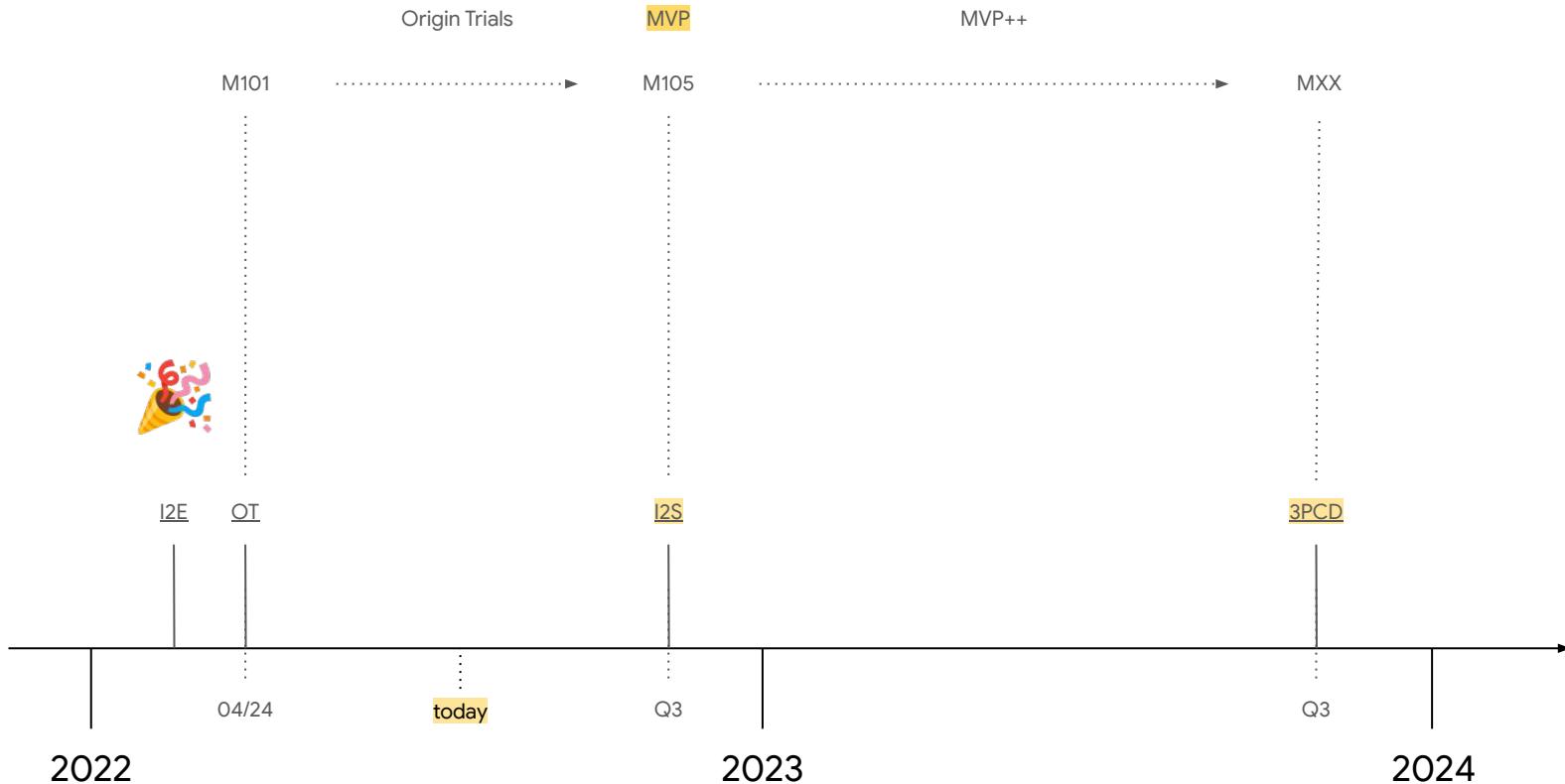
- TODO: add some slides from UX summit

Possible mobile Chrome surfaces

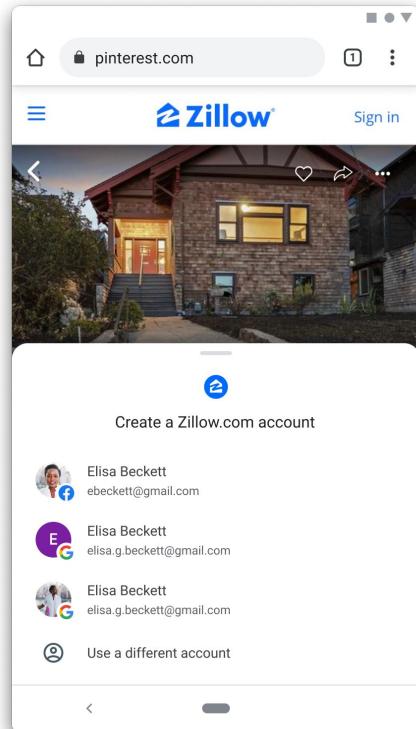


The last 3 slides (including this one) will be deleted before final submission.

Timeline



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.*