



The Web Platform, Privacy and Federation

IIW 2020

goto@chromium.org

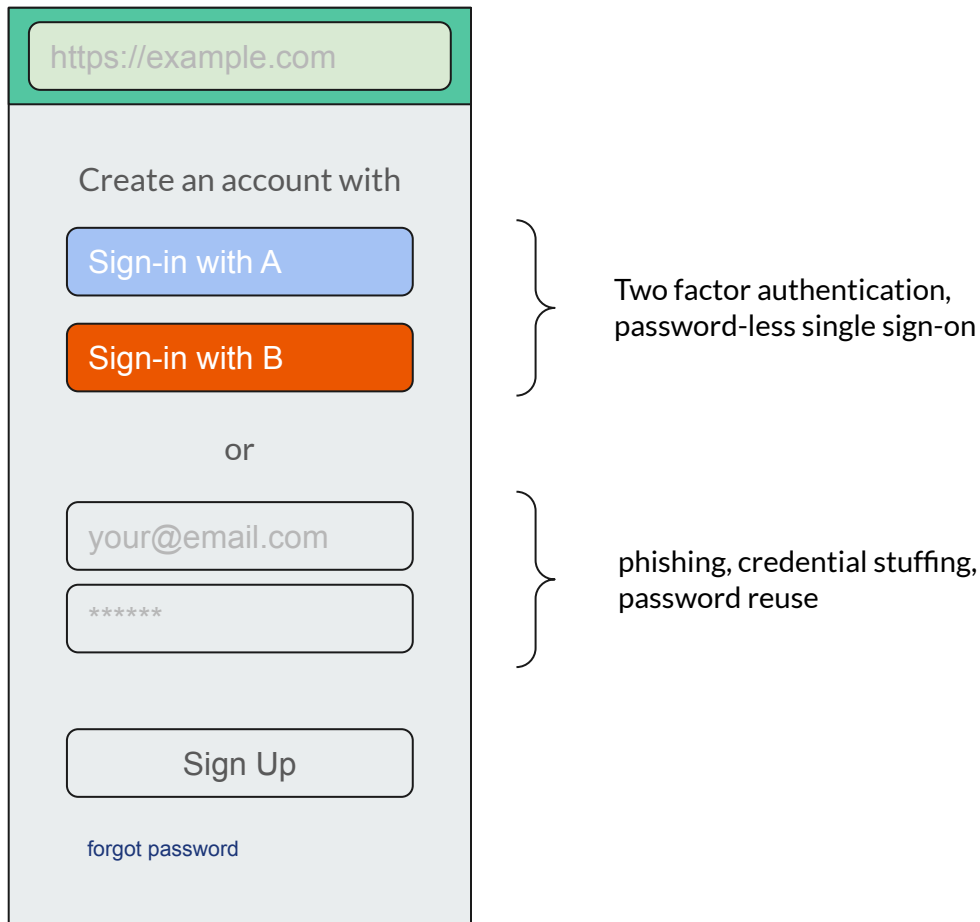


Agenda

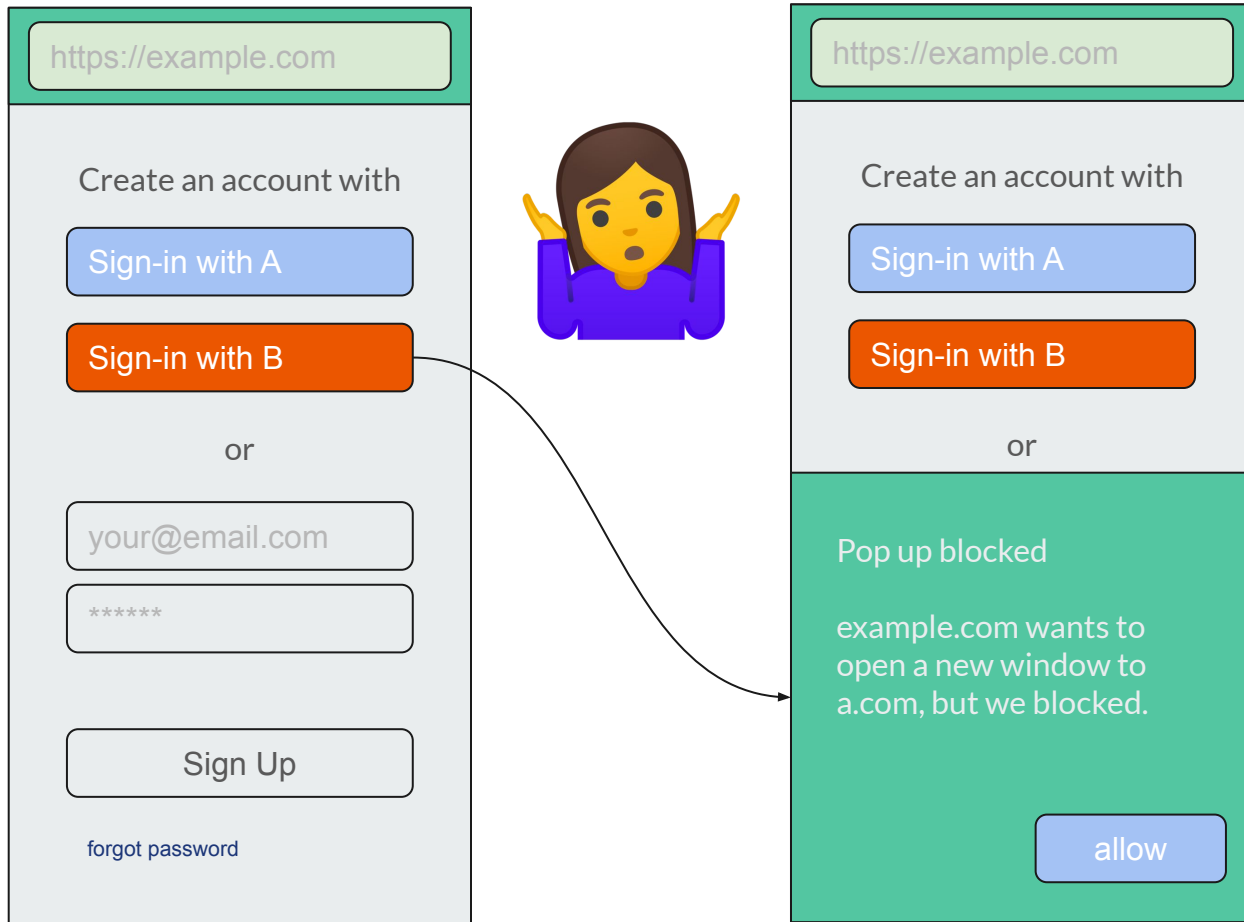
1. Premise
 - Premise: federation is good, we want to preserve it.
 - i. SSI seems interesting, but let's focus on federation for this discussion.
 - Why > What > How > Who > When
 - Users first > developers second (RPs) > frameworks (IDPs) > browser engines third > technical purity fourth
 - Cameron: Minimal disclosure for a constrained use, Justifiable Parties
2. The Why?
 - The Lowest Common Denominator problem (of general purpose primitives)
 - The Tracking Problem
 - The [Classification](#) problem
3. The What?
 - The [RP tracking](#) problem: minimal disclosure for a constrained use
 - The [IDP tracking](#) problem: justifiable parties
4. The Who: Help?
5. The When: TBD?

The Why

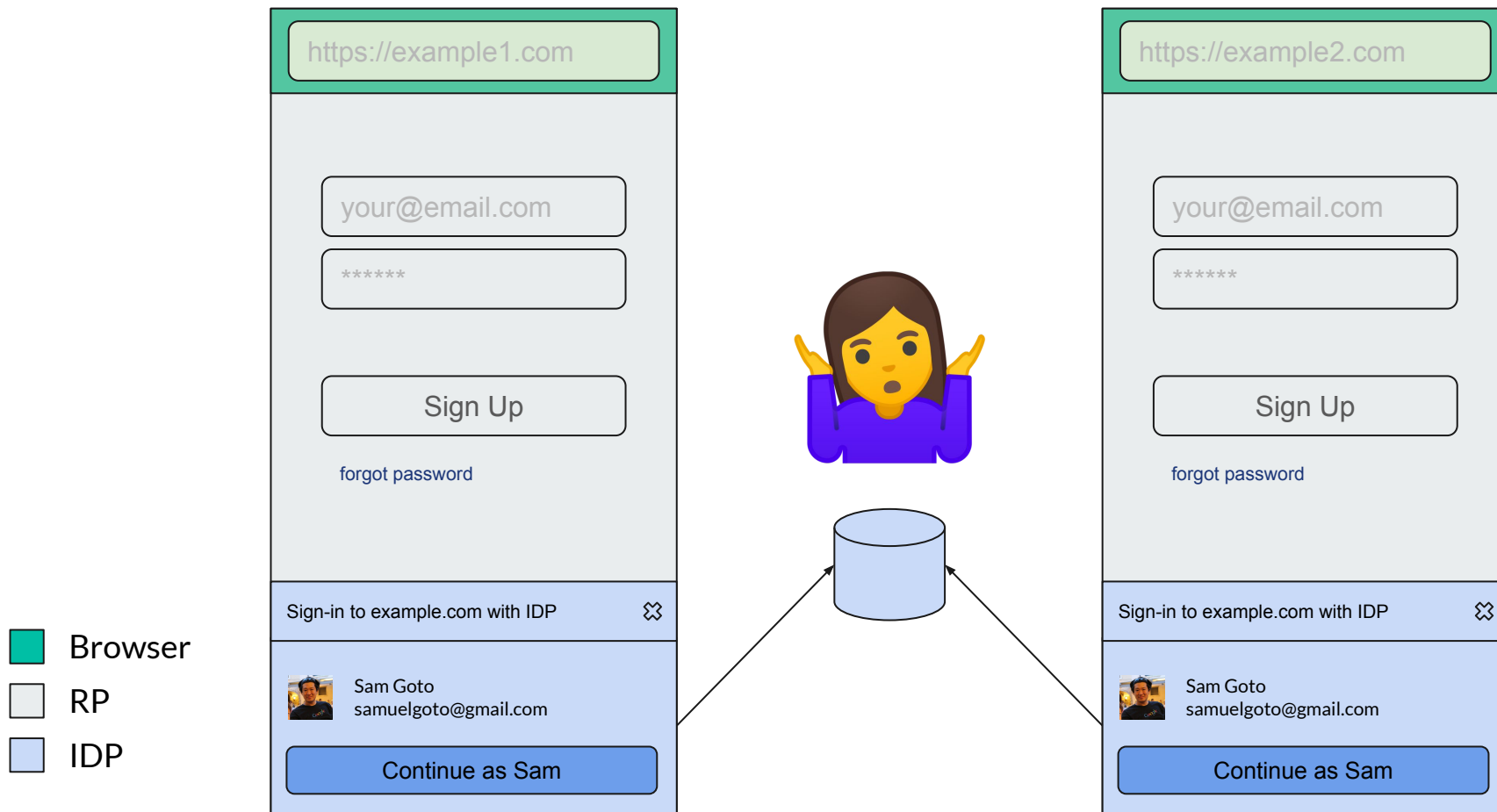
Federation is Safer Than Usernames/Passwords



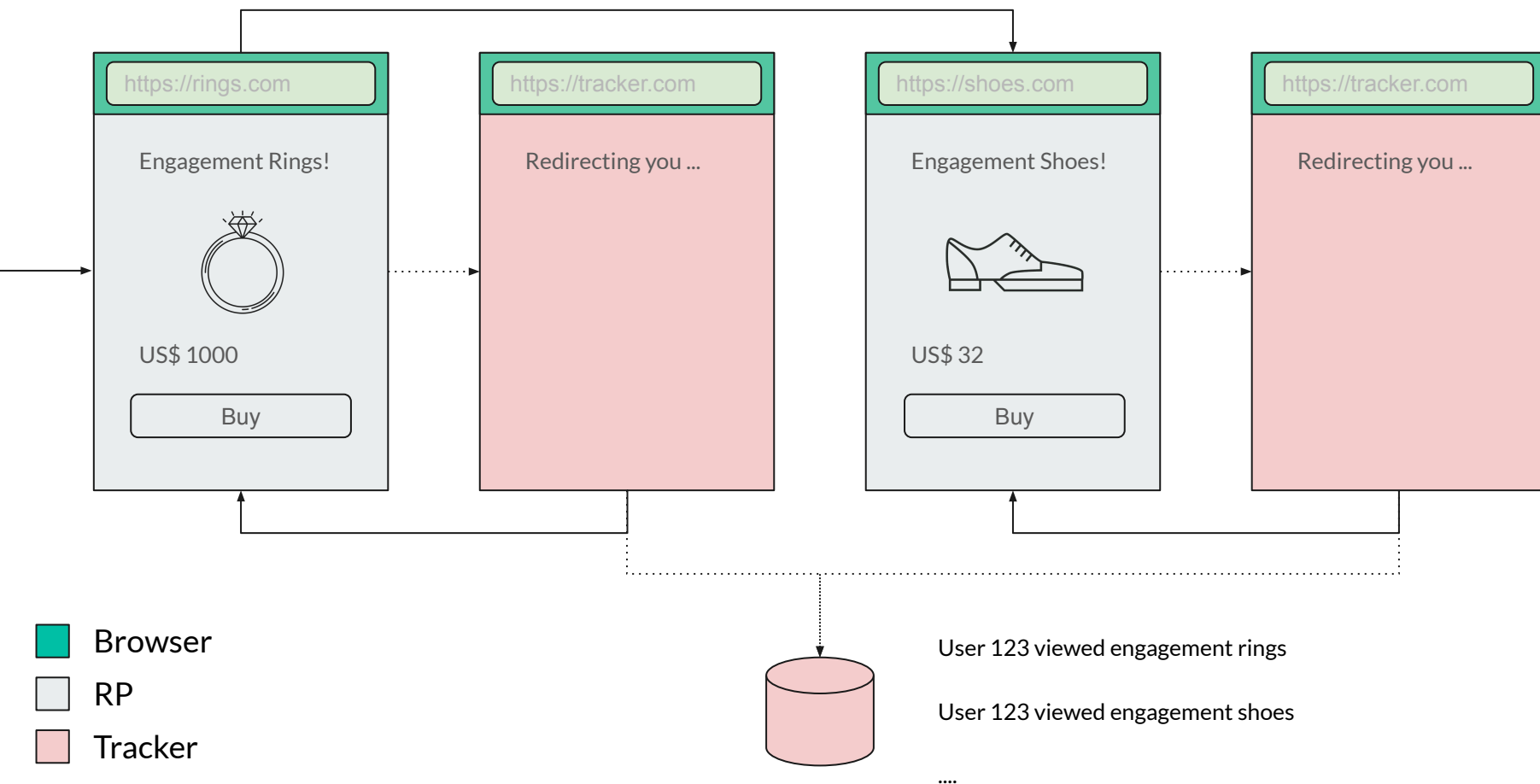
The Lowest Common Denominator Problem (of general purpose primitives)



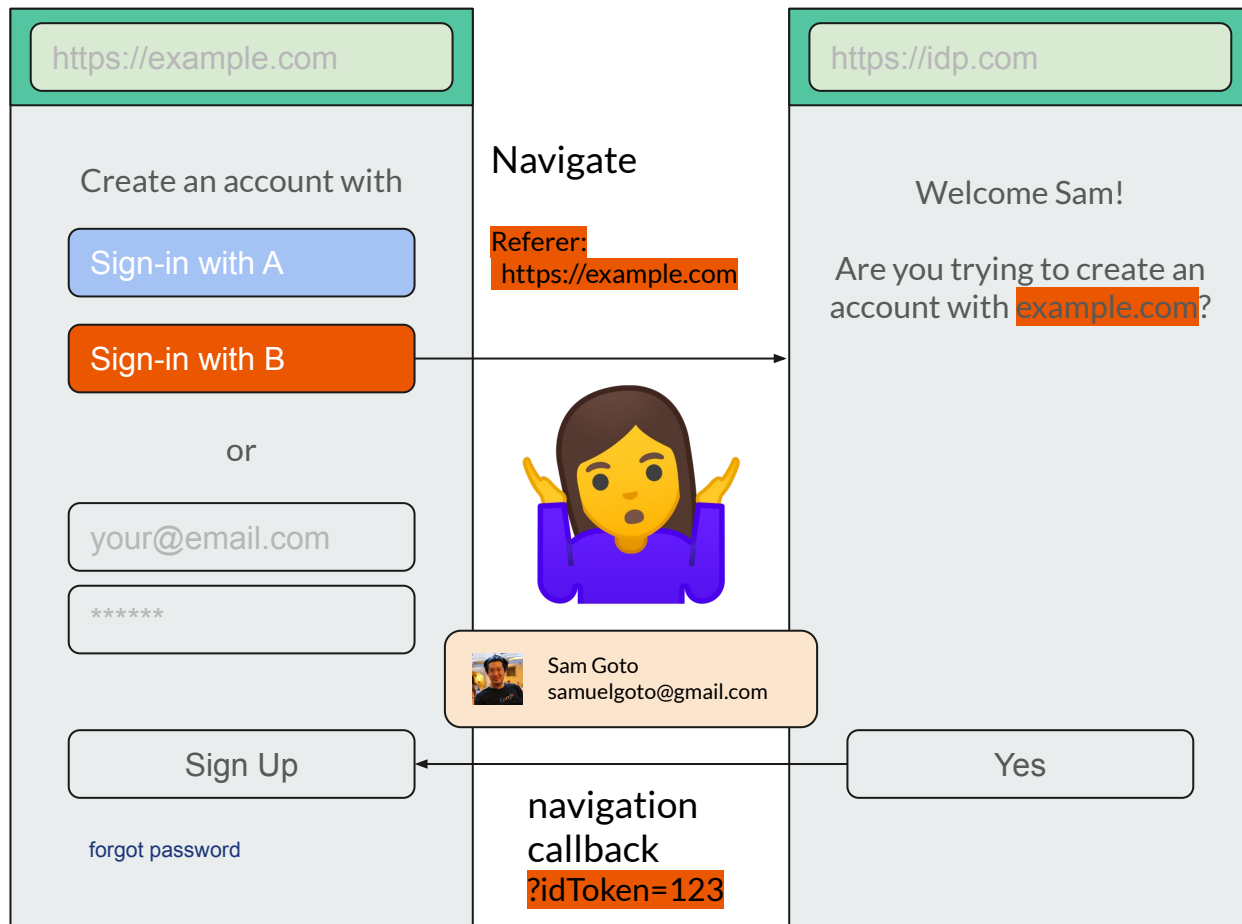
The <iframe>s and 3P Cookie Classification Problem



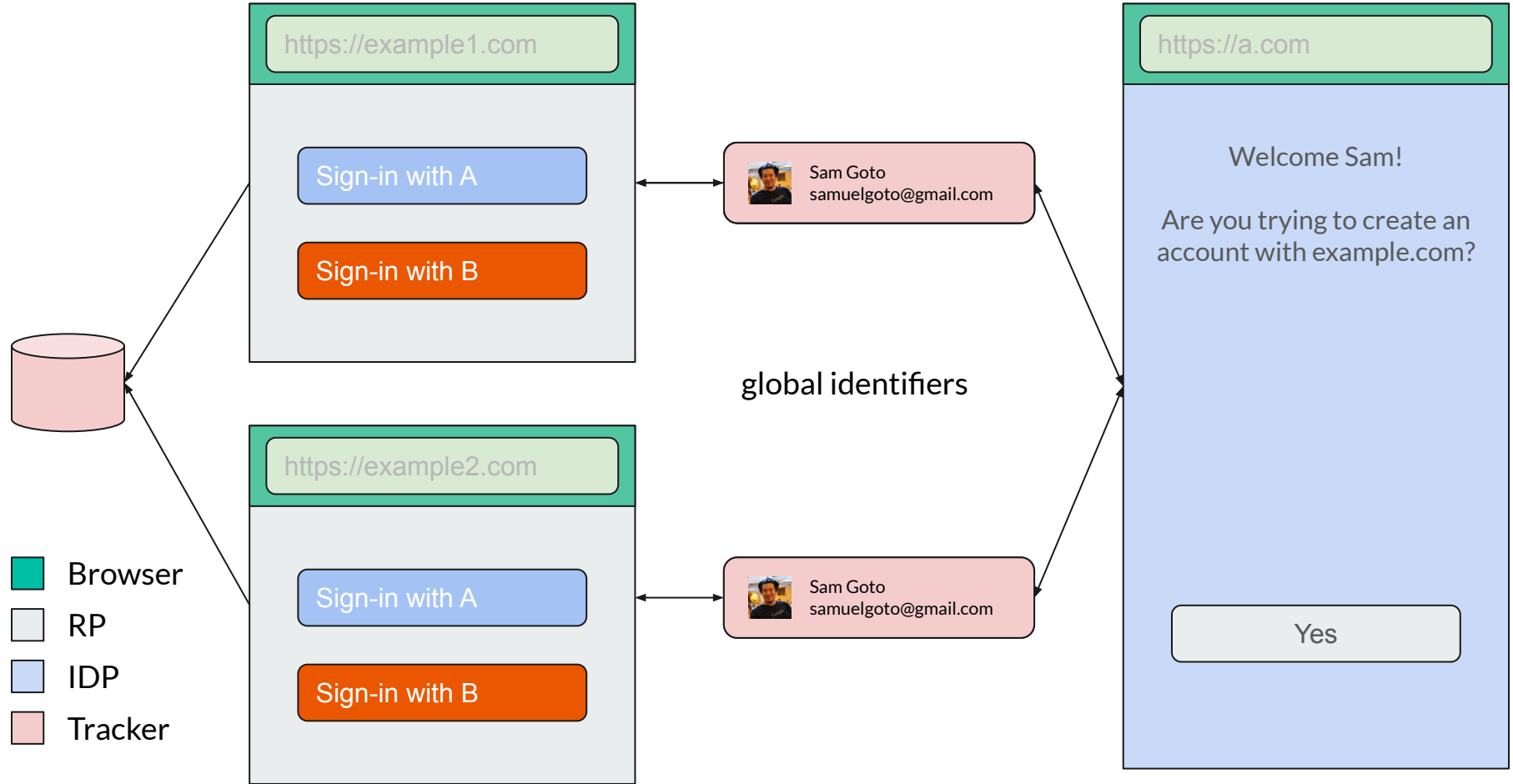
Navigational/Bounce Tracking and Link Decoration



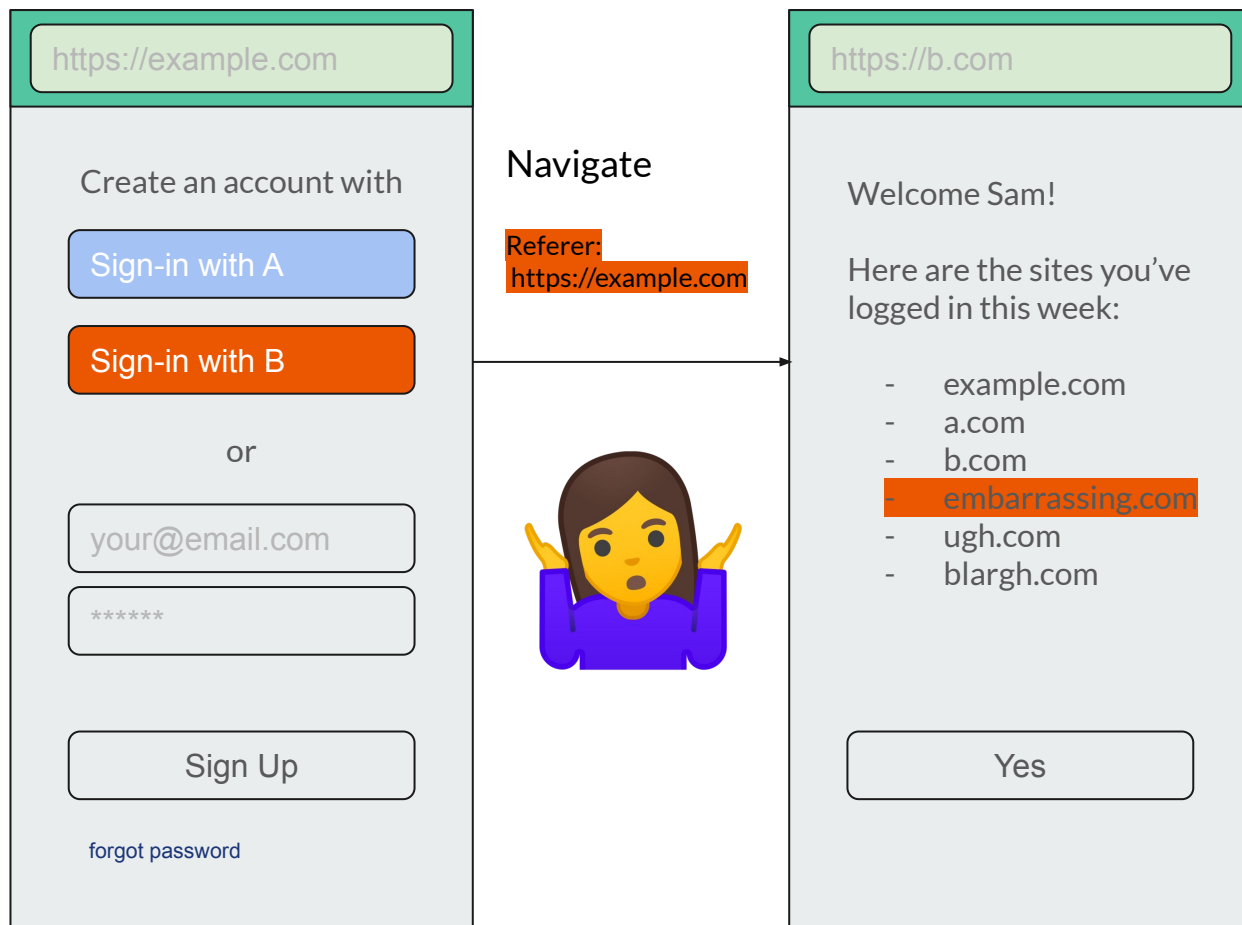
The Classification Problem



The (Unintentional) RP Tracking Problem



The (Unintentional) IDP Tracking Problem



The What Not

Enterprise Policies



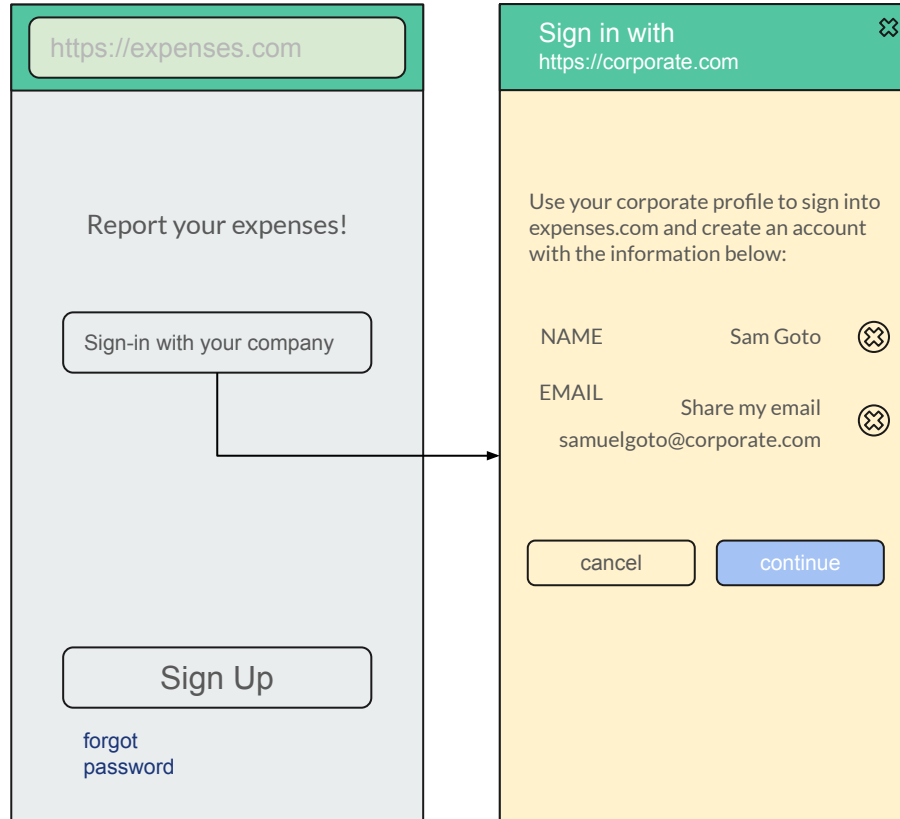
UA



IDP



RP

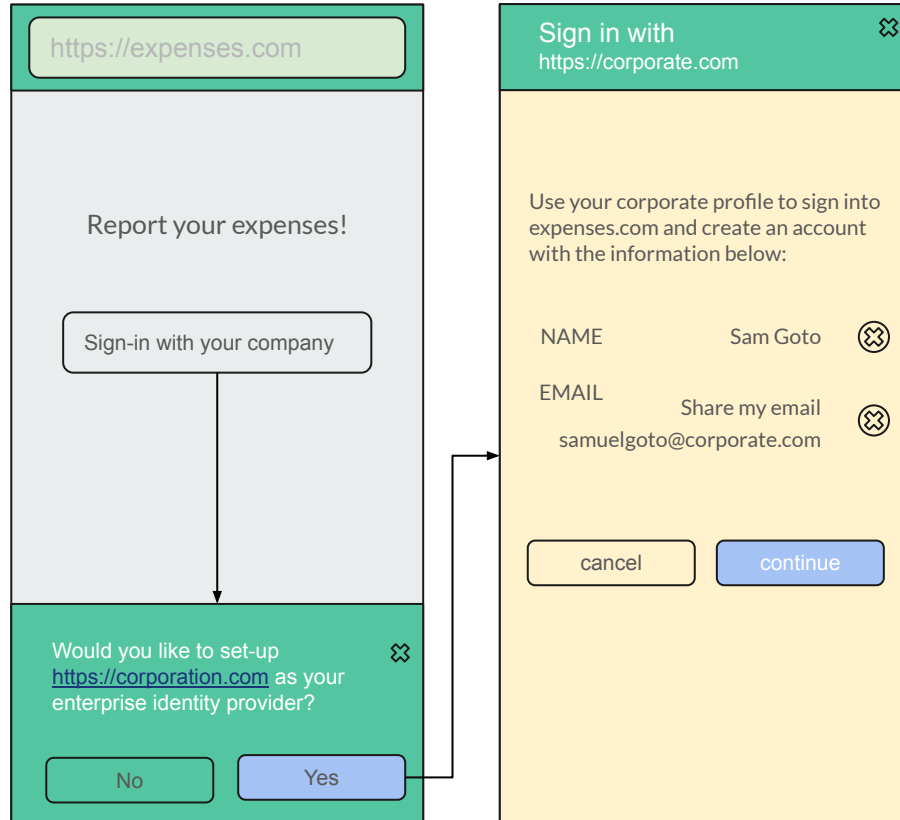


Enterprise BYOD

 UA

 IDP

 RP



The What

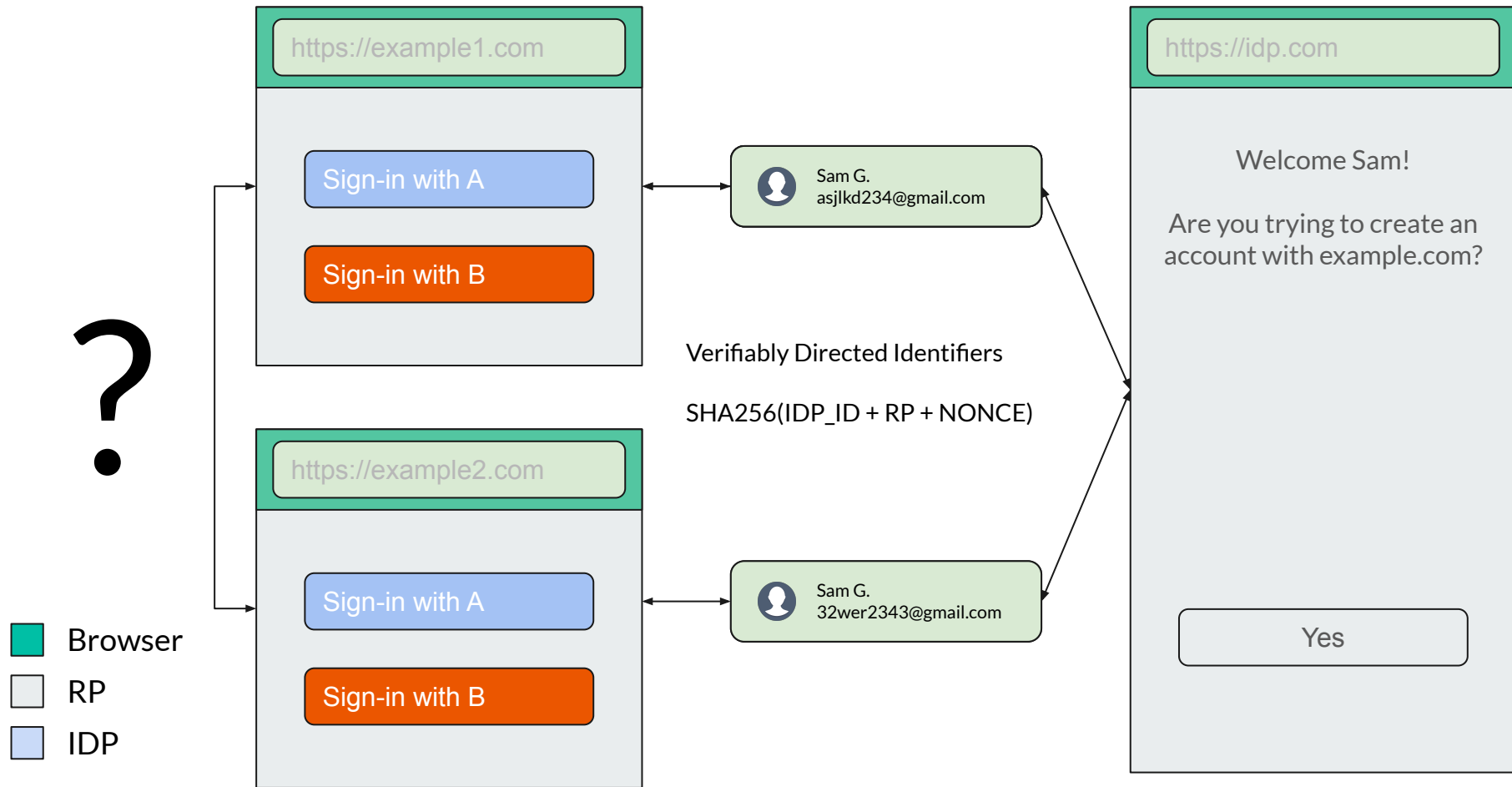
The RP Tracking Problem

Correlation

Cameron's 7 Laws of Identity

- 1) User Control and Consent
- 2) **Minimal Disclosure for a Constrained Use**
- 3) Justifiable Parties
- 4) **Directed Identity**
- 5) Pluralism of Operators and Technologies
- 6) Human Integration
- 7) Consistent Experience Across Contexts

Mitigating the RP Tracking Problem



Sign-In / Sign-Up



Alternatives under consideration

- Alternatives under consideration
 - The Permission-oriented Variation
 - The Mediation-oriented Variation
 - The Delegation-oriented Variation
- Trade-offs



UA

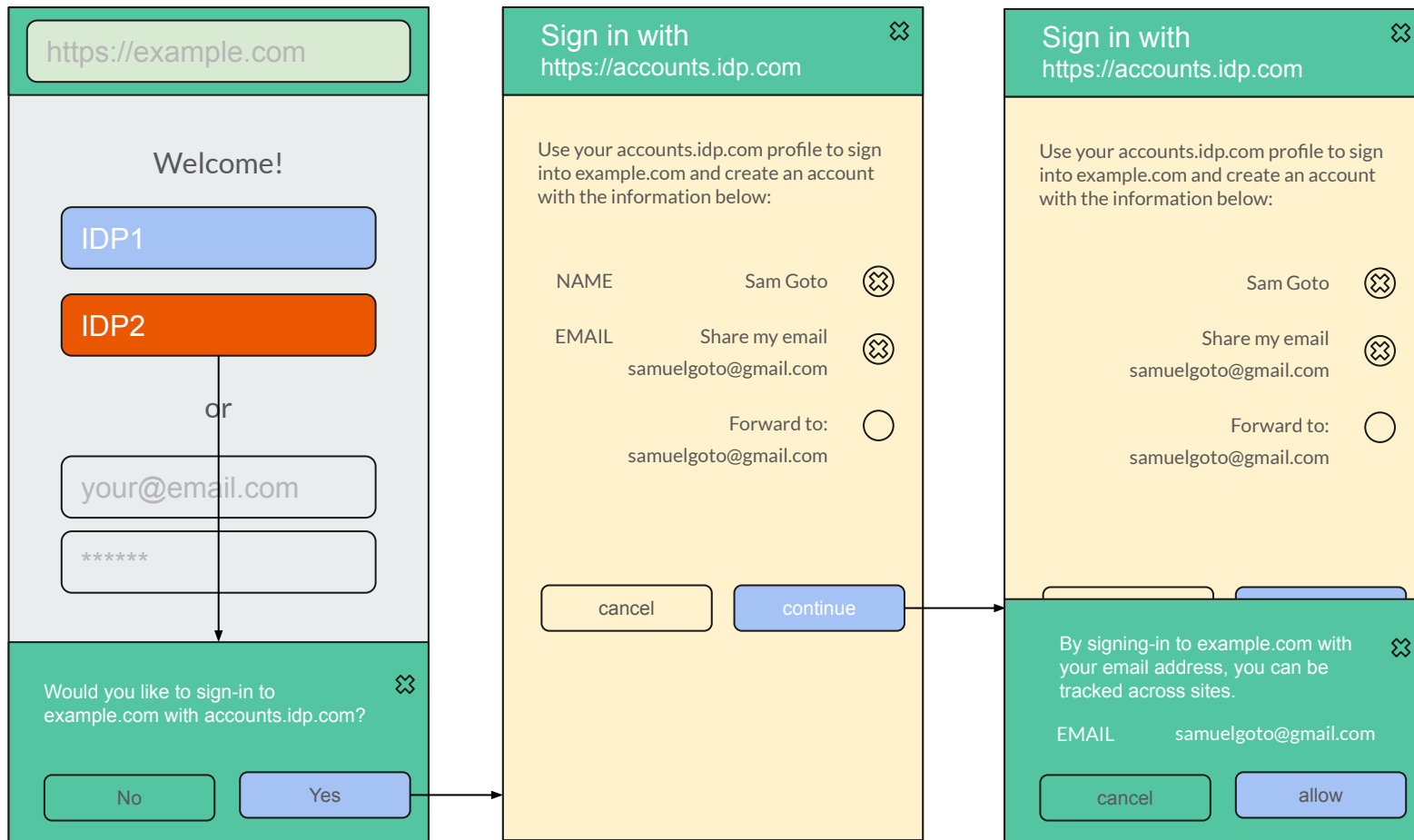


IDP



RP

#1 The Permission-oriented Variation





User Agent

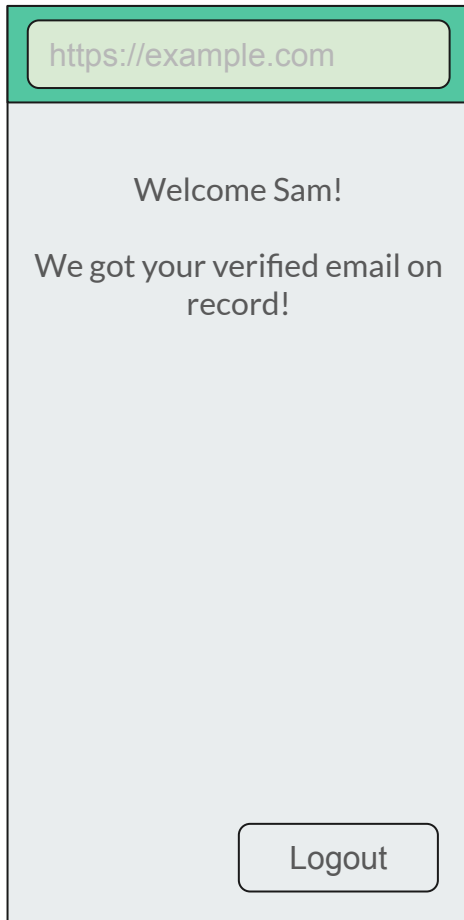


Relying Party

#2 The Mediation-oriented Variation






Server-Side Relying Party Backwards Compatibility



If the user grants access, the id token is passed back to the application:

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "iss": "https://accounts.a.com",
  "sub": "110169484474386276334",
  "aud": "https://example.com",
  "name": "Sam",
  "given_name": "Sam",
  "family_name": "G.",
  "email": "242423asf390@gmail.com",
  "email_verified": "true",
}
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  SECRET
)
```

-  Browser
-  RP
-  IDP

Authorization

Authorization



UA



IDP



RP

<https://example.com>

Welcome! Sync your external calendar with us!

Sync your calendar!


Would you like to connect your accounts.idp.com calendar with example.com?

No

Yes

Sign in with <https://accounts.idp.com>

Authorize example.com to read your calendar?


 read your calendar

cancel

continue

Sign in with <https://accounts.idp.com>

Authorize example.com to read your calendar?

 read your calendar

cancel

continue

By authorizing example.com to access your calendar, you can be tracked across sites.

cancel

allow

The IDP Tracking Problem

Phone-homing

Cameron's 7 Laws of Identity

- 1) User Control and Consent
- 2) Minimal Disclosure for a Constrained Use
- 3) **Justifiable Parties**
- 4) Directed Identity
- 5) Pluralism of Operators and Technologies
- 6) Human Integration
- 7) Consistent Experience Across Contexts



UA

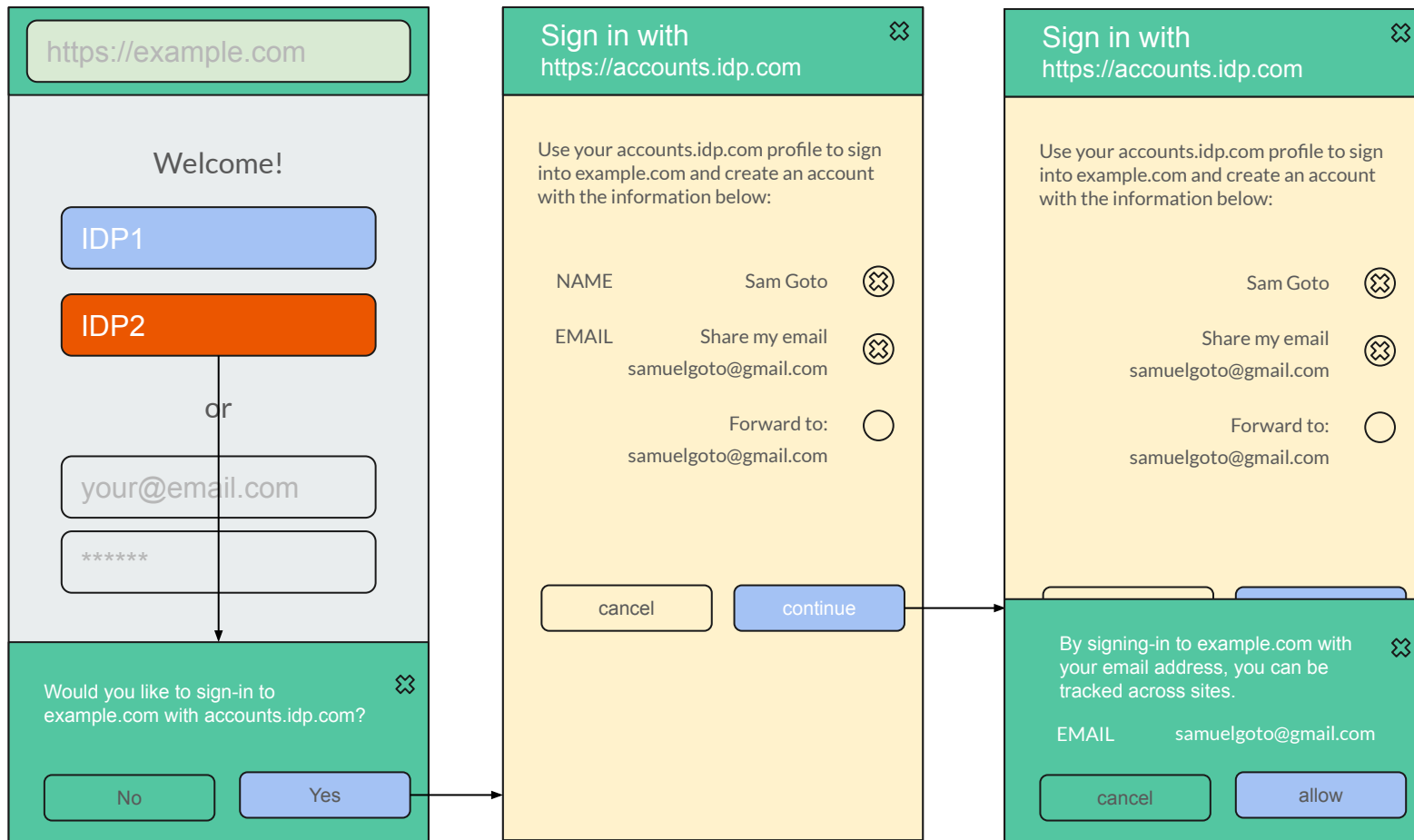


IDP



RP

#1 The Permission-oriented Variation





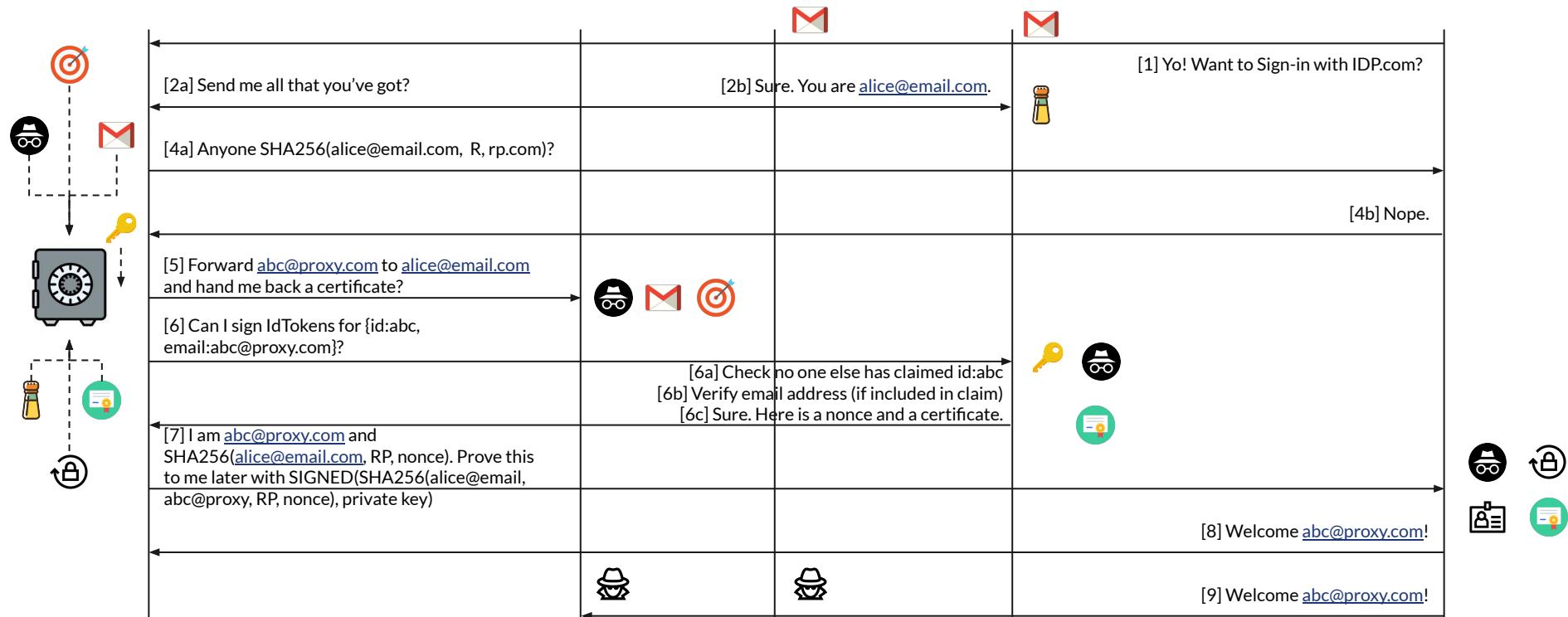
User Agent

Email Proxy
(proxy.com)

Email Provider
(email.com)

Identity Provider
(idp.com)

Relying Party
(rp.com)



#3 The Delegation-oriented Variation



global email



directed email



keypair



certificate



nonce



recovery token

Help?



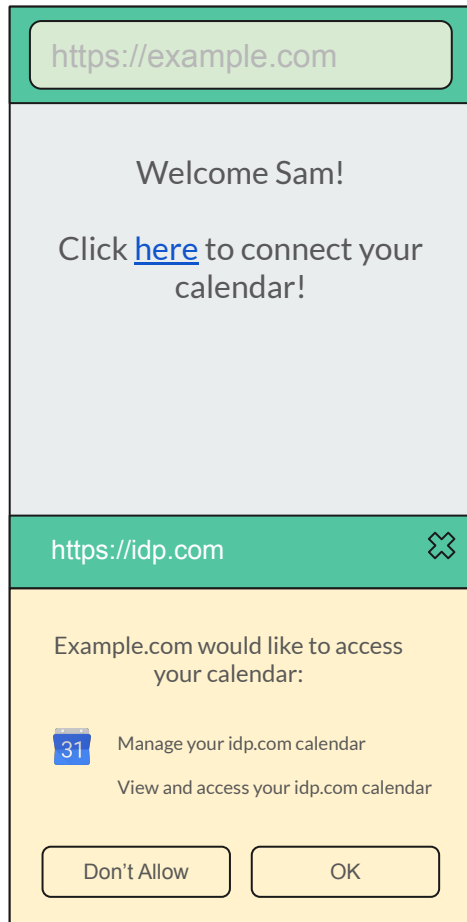
Way more questions than answers

- Other Problems With Federation
 - The IDP Impersonation Problem
 - The Portability Problem
 - The NASCAR flag Problem
- Ecosystem Design
 - Can RPs do their job well enough with directed identifiers? Customer support.
- Technical Design
 - Is the RP tracking problem and the IDP tracking problem mutually exclusive?
 - To what extent can we programmatically enforce directed identifiers?
 - How does authorization work?
- Product Design
 - Should enterprise policies play a role in setting a different privacy bar for [enterprise SSO](#)?
 - Should first party sets play a role in setting a different privacy bar for [first party SSO](#)?

ANNEX

—

Identification, Authentication and Authorization?



Browser UI

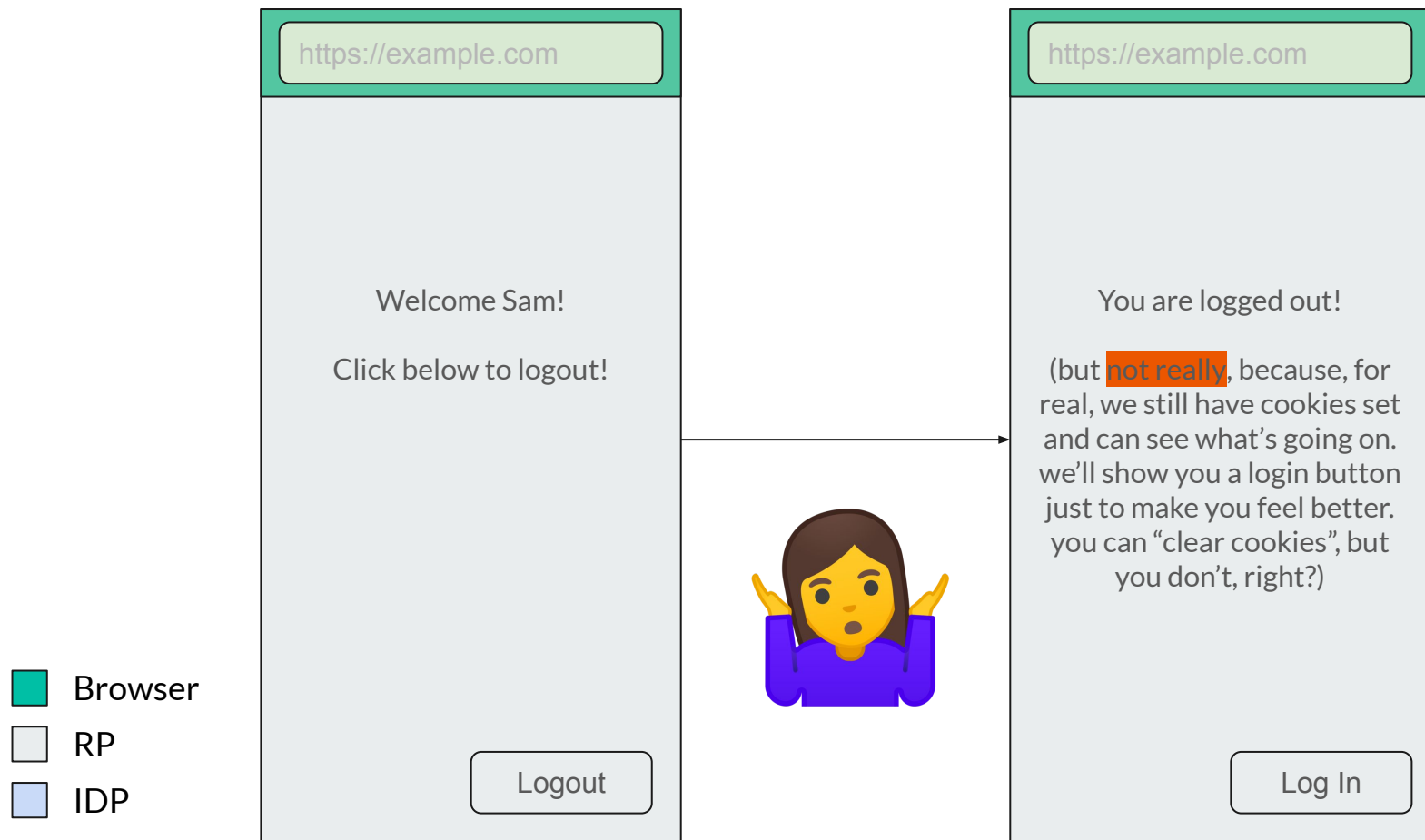


IDP UI

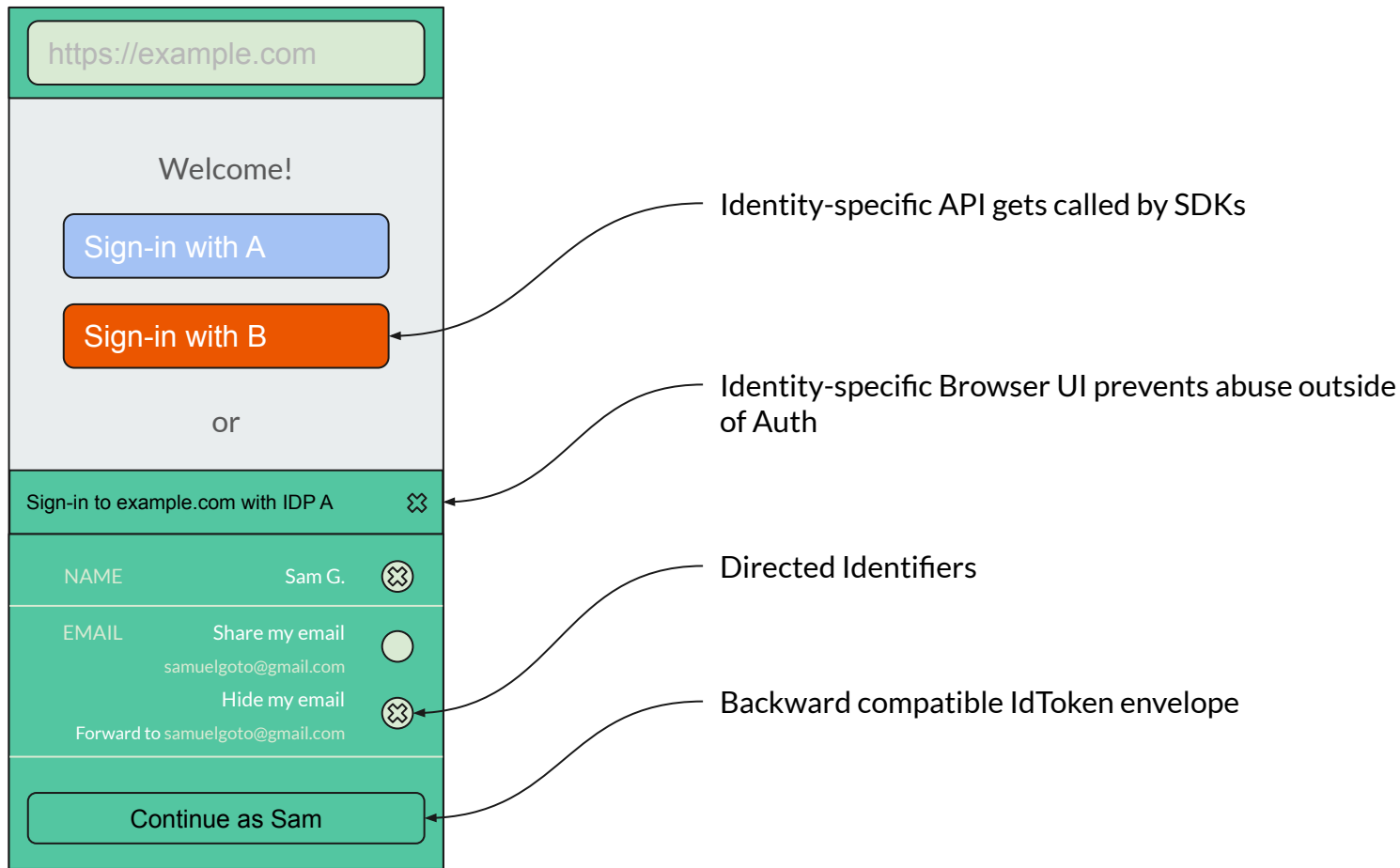


RP UI

The First Party Tracking Problem

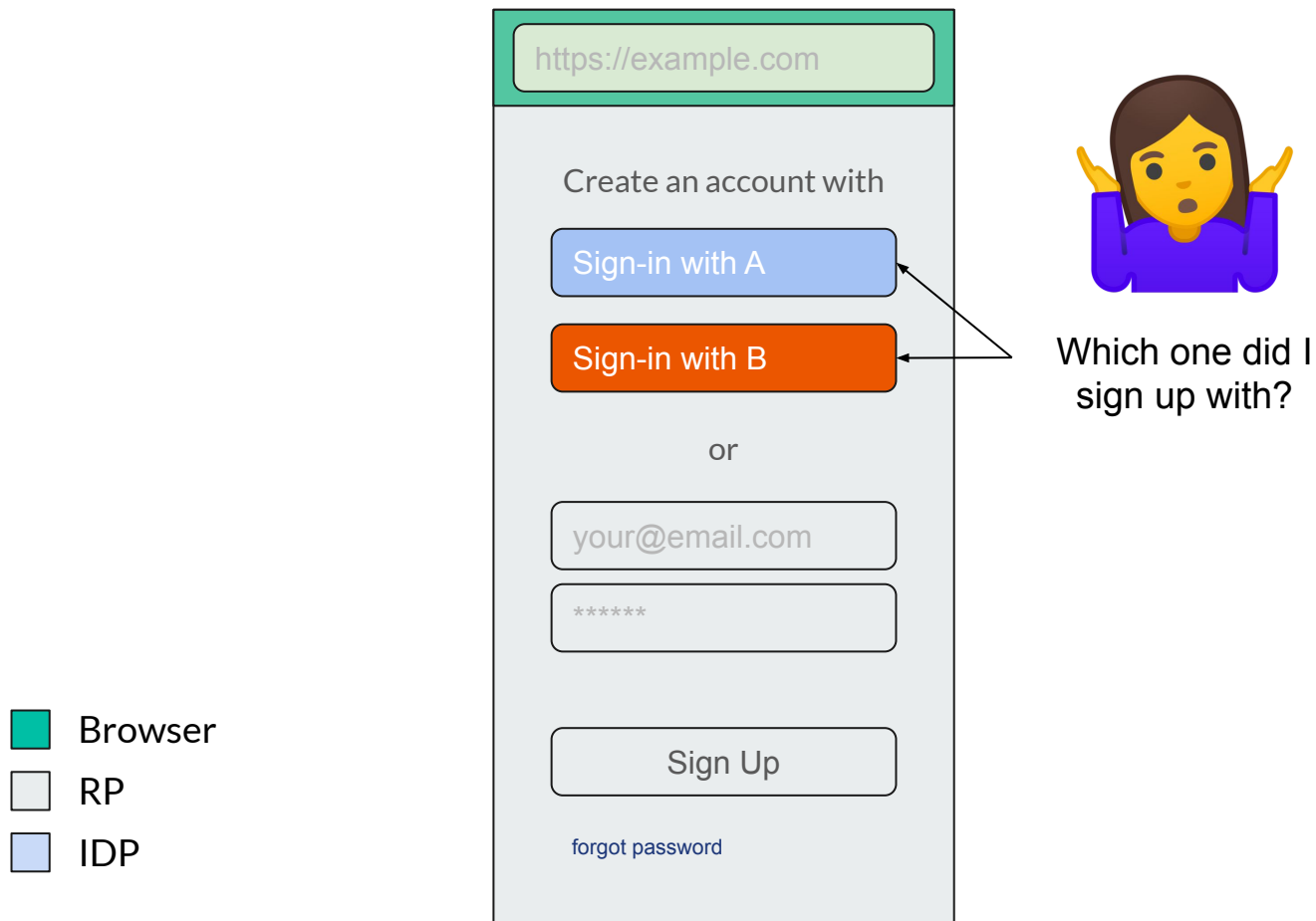


Mitigating the Classification Problem



This deck is shared publicly.

The NASCAR Flag Problem



Activation Vehicle

The activation **intervention point** most identity providers provide an sdk.js library that is pulled from the O(M) relying parties. **Recompile that**, and you'll activate O(M) websites and O(B) users with a flip of a switch.

O(B)

Users

O(M)

Relying Parties

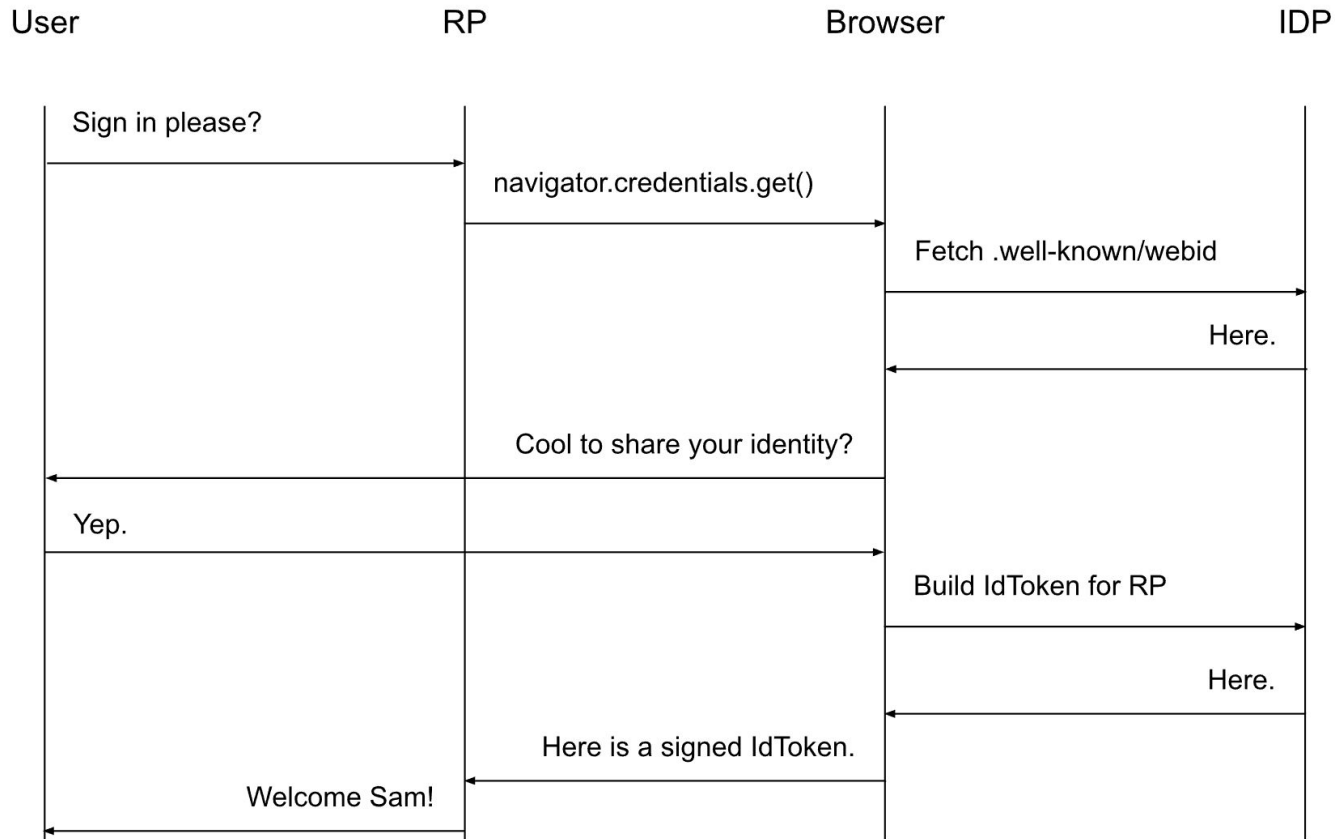


O(6)

Identity Providers

```
<script src="https://signin.a.com/signin/sdk.js"></script>
```

Potential Data Flow





Help?

1. Way more questions than answers
2. We are still trying to understand the problem space
3. Federation is safer/easier than usernames/passwords
4. General Purpose Affordances, General Purpose permissions
5. Help?

goto@chromium.org

<https://twitter.com/samuelgoto>



Premise

1. Way more questions than answers.
2. We are still trying to understand the problem space
3. Federation is safer/easier than usernames/passwords
4. General Purpose Affordances, General Purpose permissions
5. Help?