



WebID

TPAC 2020

Ken Buchanan (kenrb@google.com)

Majid Valipour (majidvp@google.com)

Sam Goto (goto@google.com)



<https://wicg.github.io/WebID>

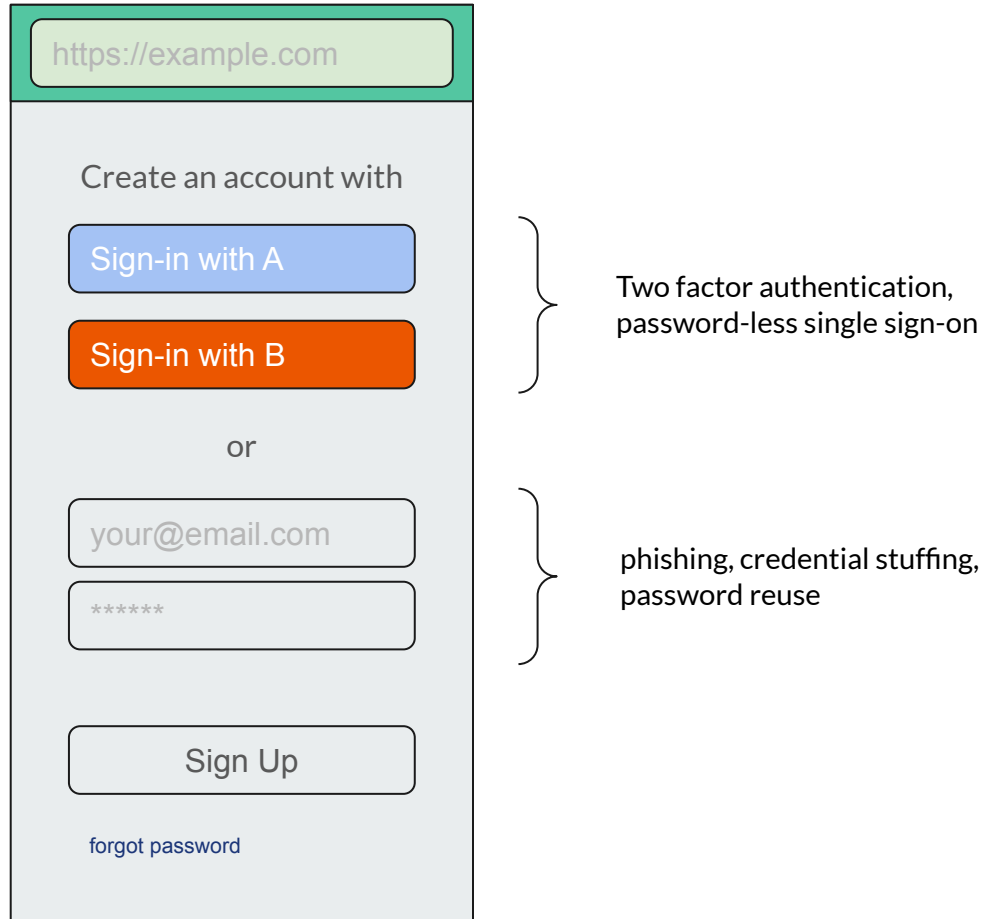


Agenda

- The Problem
 - Premise: federation is good, we want to preserve it.
 - How federation works
 - User activity tracking on the web
 - Scope of this project
- Solution Framework
 - Directed identifiers
 - High-level approaches for an identity API
- Moving Forward
 - Challenges
 - Community engagement

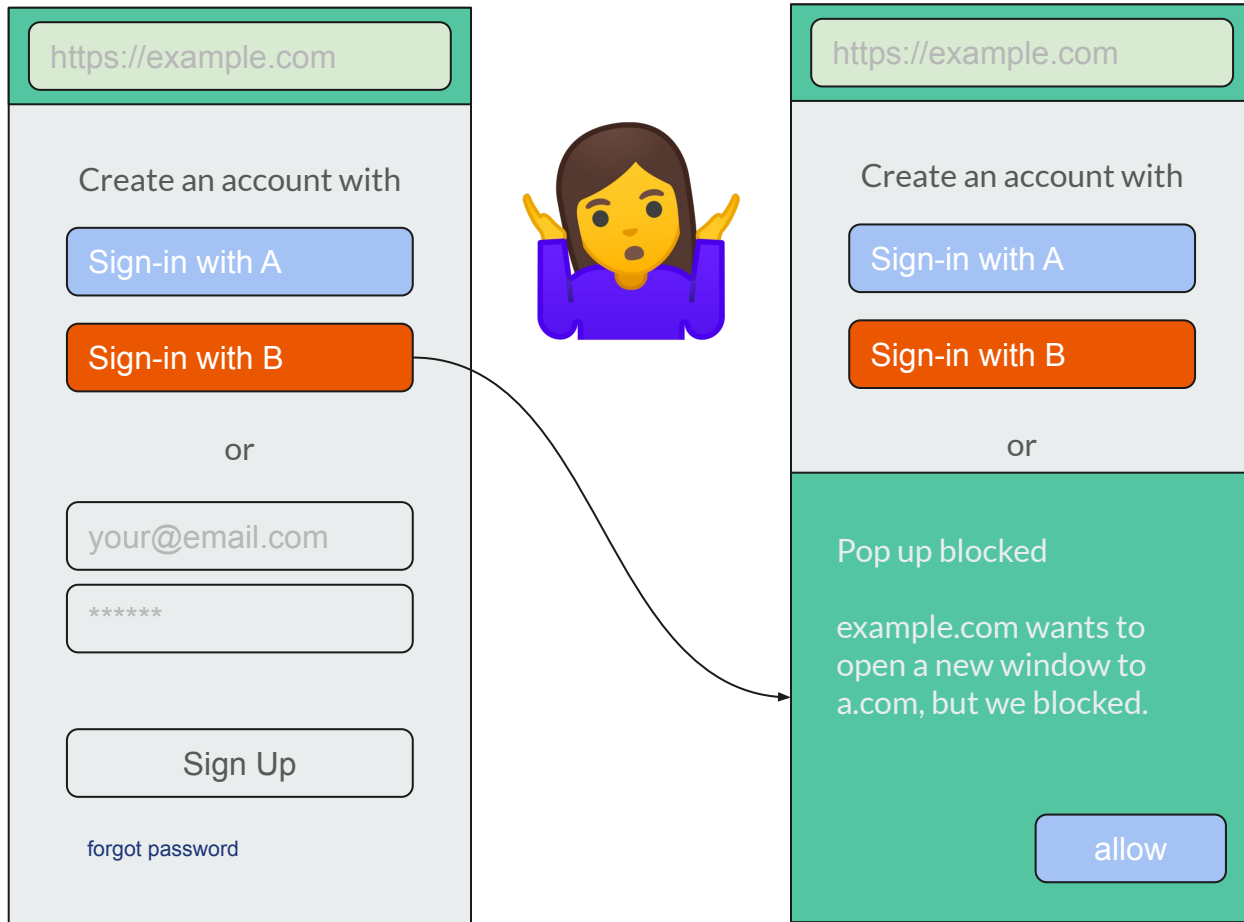
The Problem

Federation is Safer Than Usernames/Passwords



- Browser
- RP
- IDP




Reliance on General-purpose Web Primitives

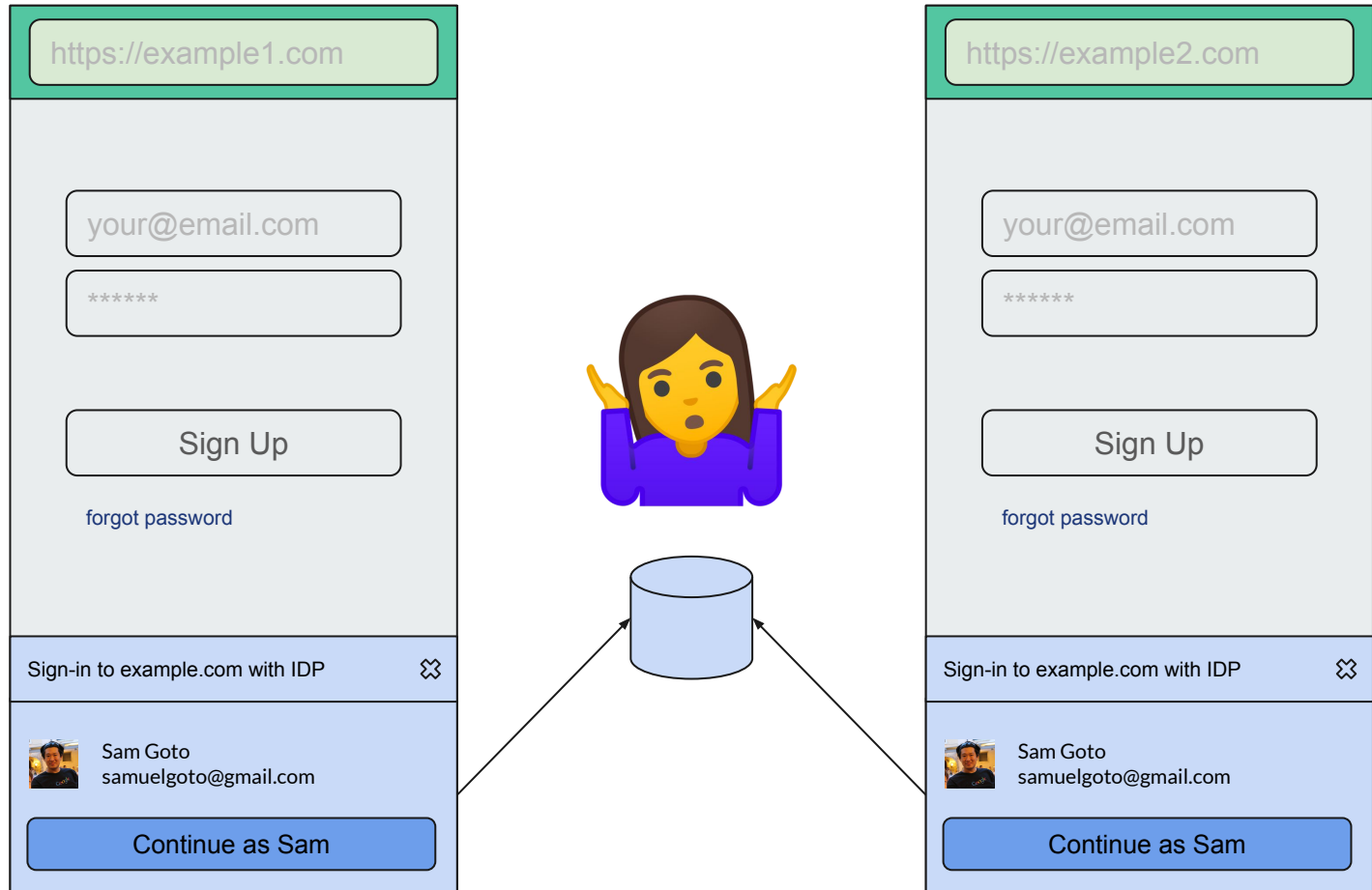


Other low level primitives:

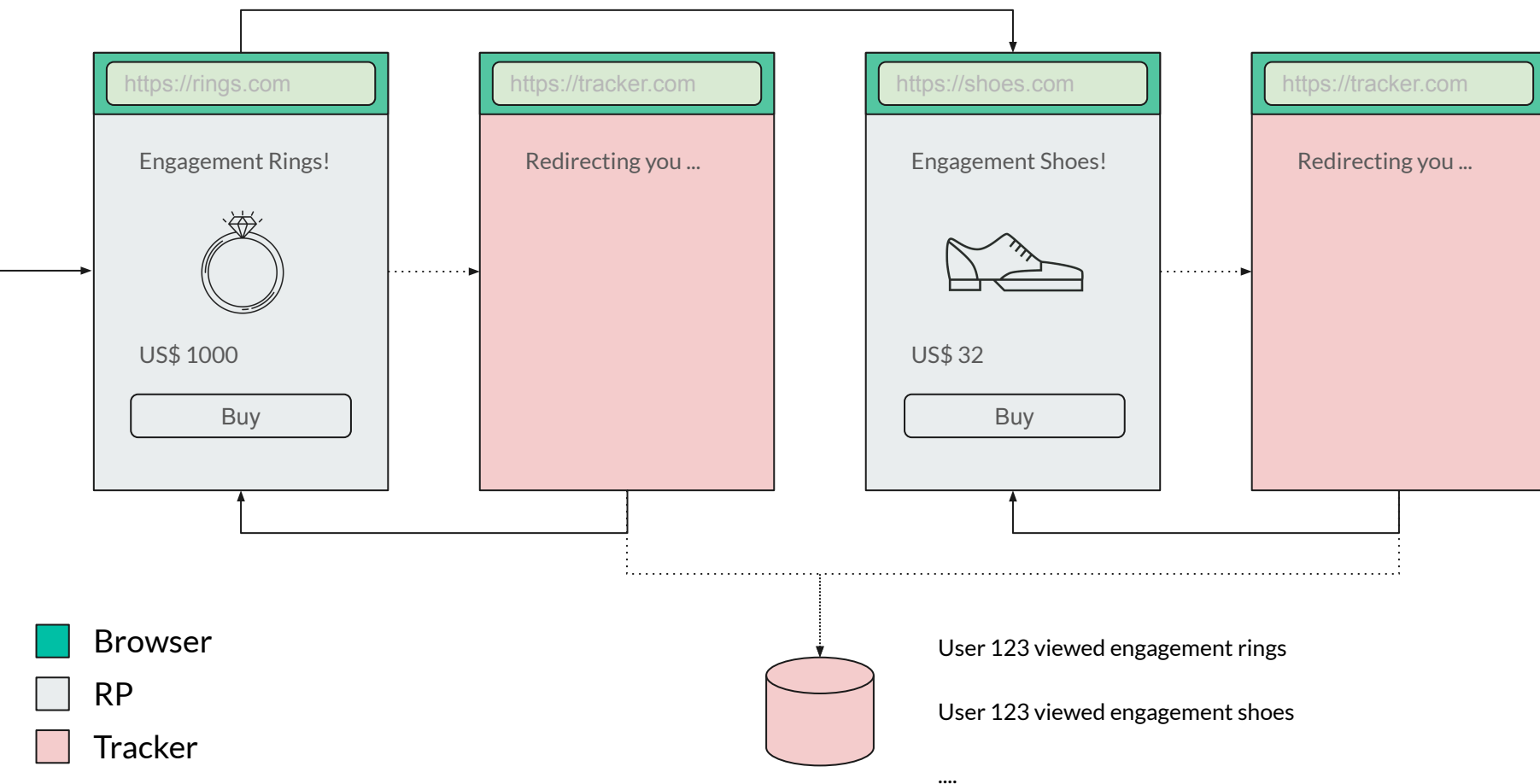
- Iframes
- Cookies
- Redirects
- Pop-ups
- URL Parameters

Third-Party Cookie Access

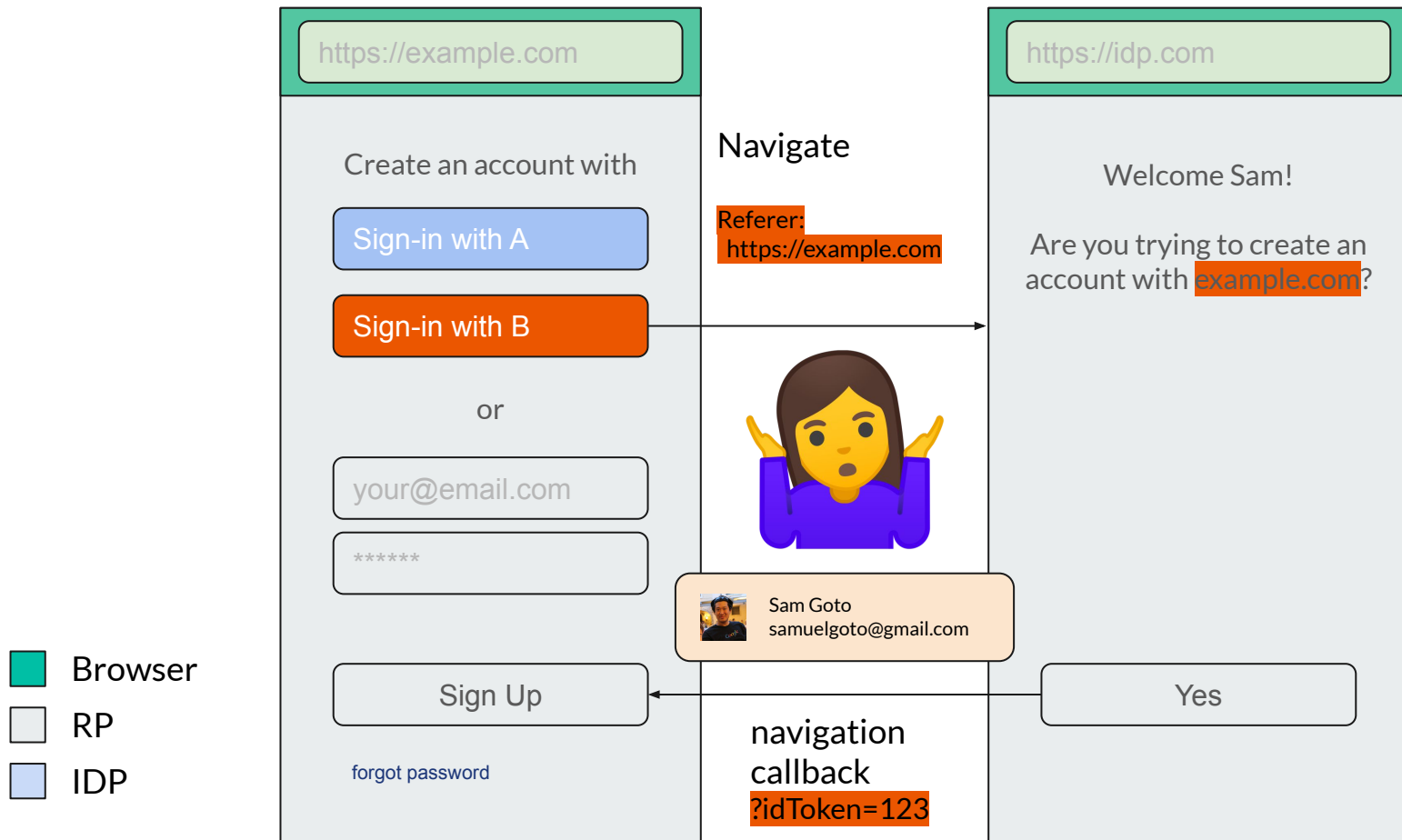
-  Browser
-  RP
-  IDP



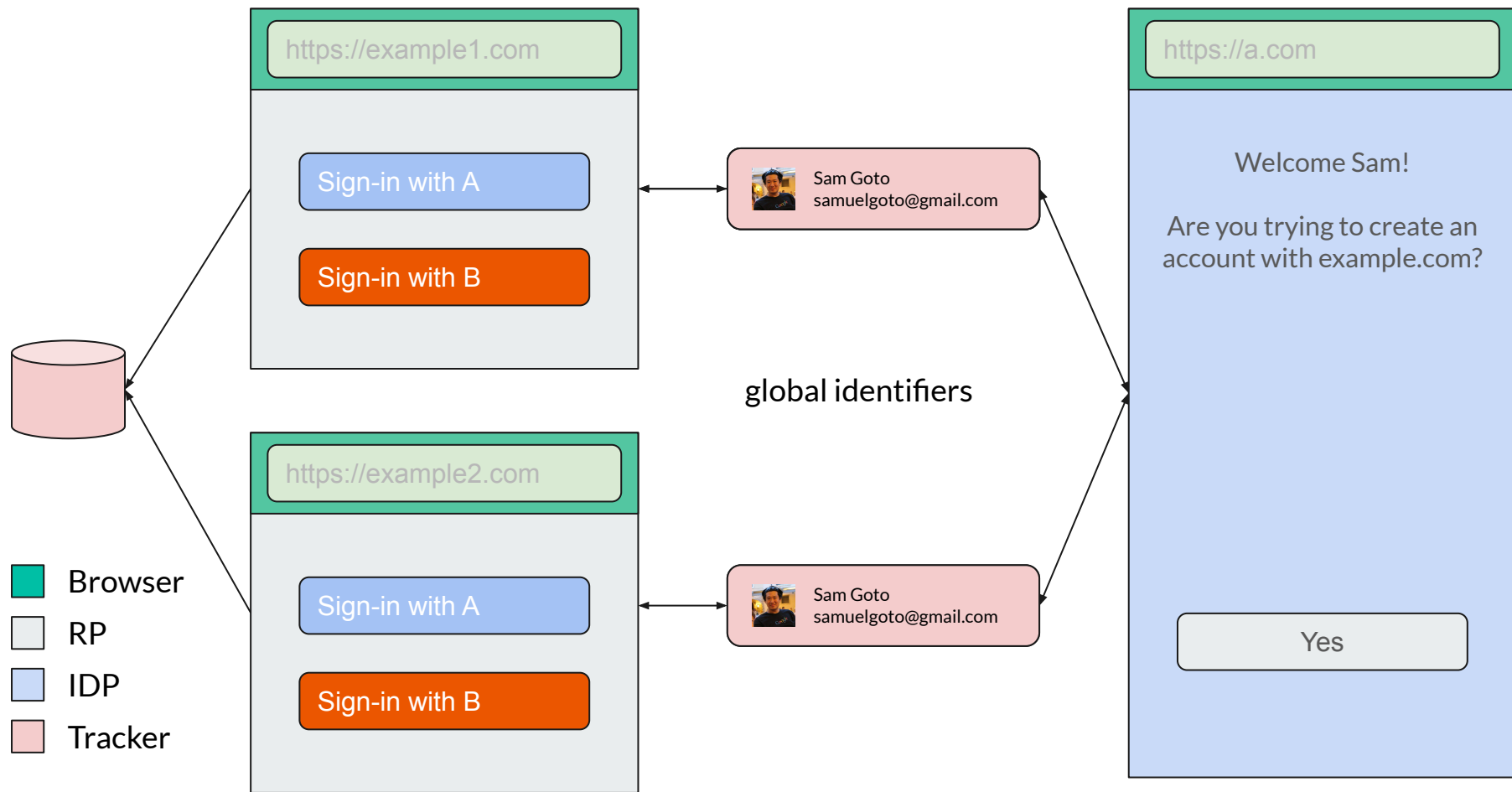
Navigational/Bounce Tracking and Link Decoration



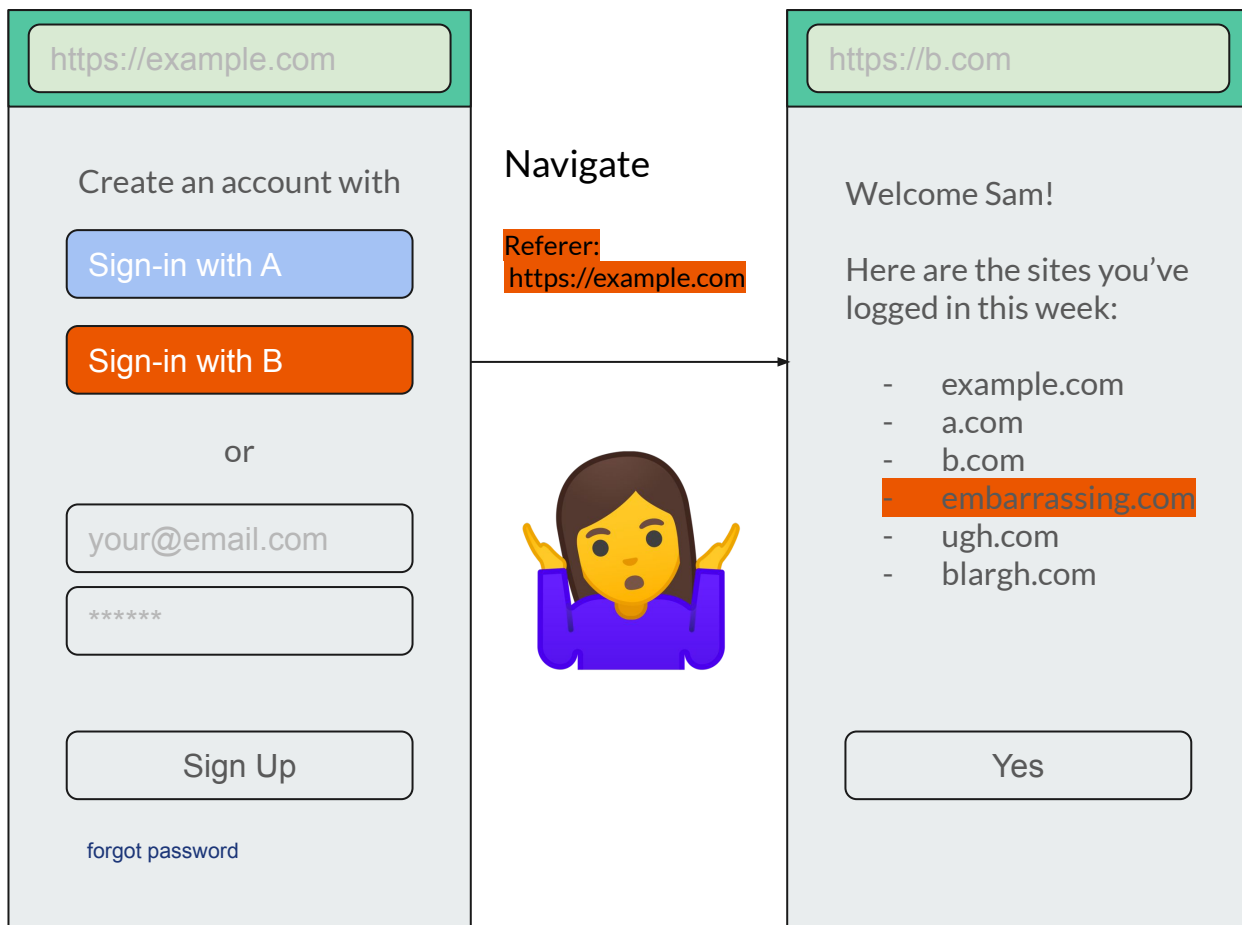
The Classification Problem



RP Consequences of Web Identity



IDP Consequences of Federated Sign-in



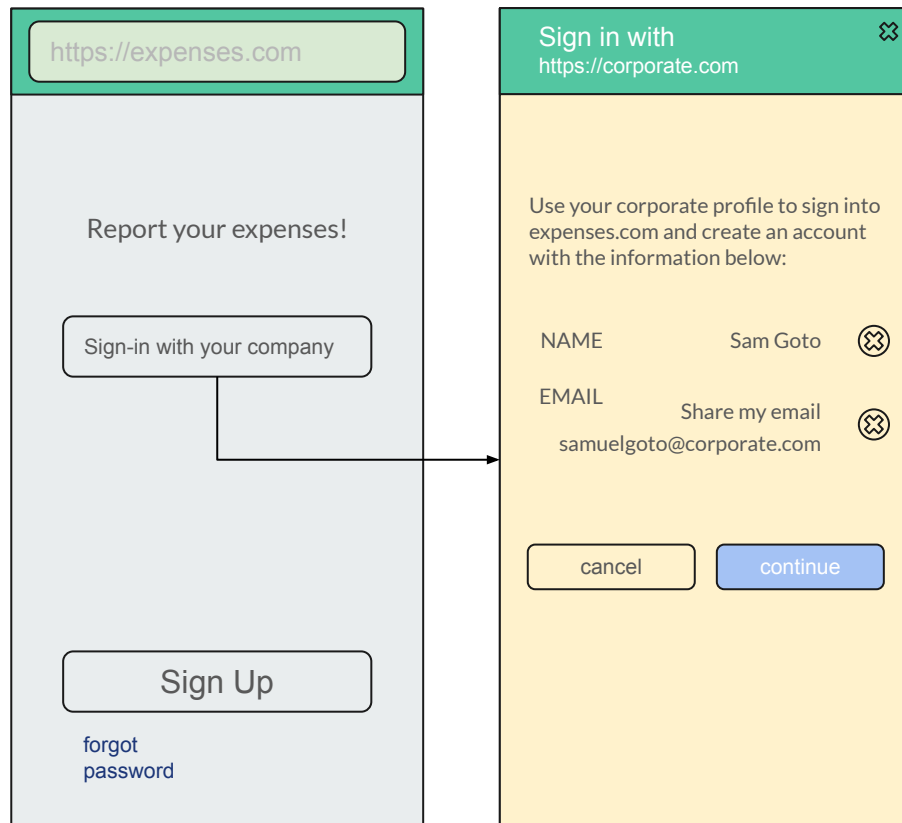
Scope and Limitations



Currently out of scope

- IDP Impersonation
- Cross-device sign-in state
- The “NASCAR flag” problem

Enterprise Use Cases



WebID Proposals for Sign-In / Sign-Up

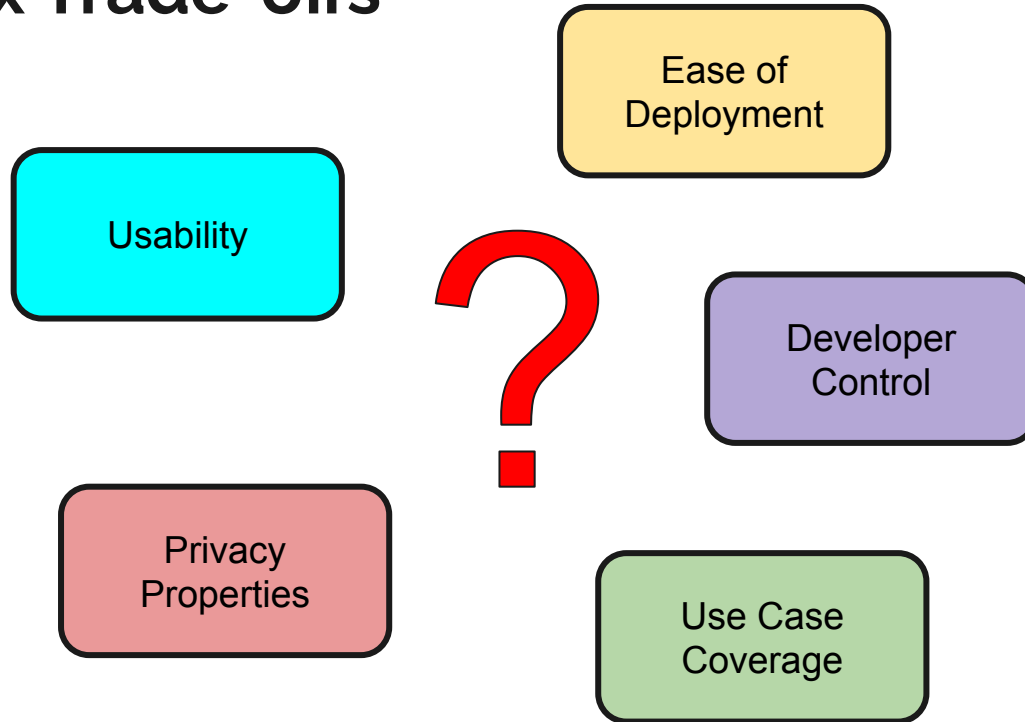


Important caveat

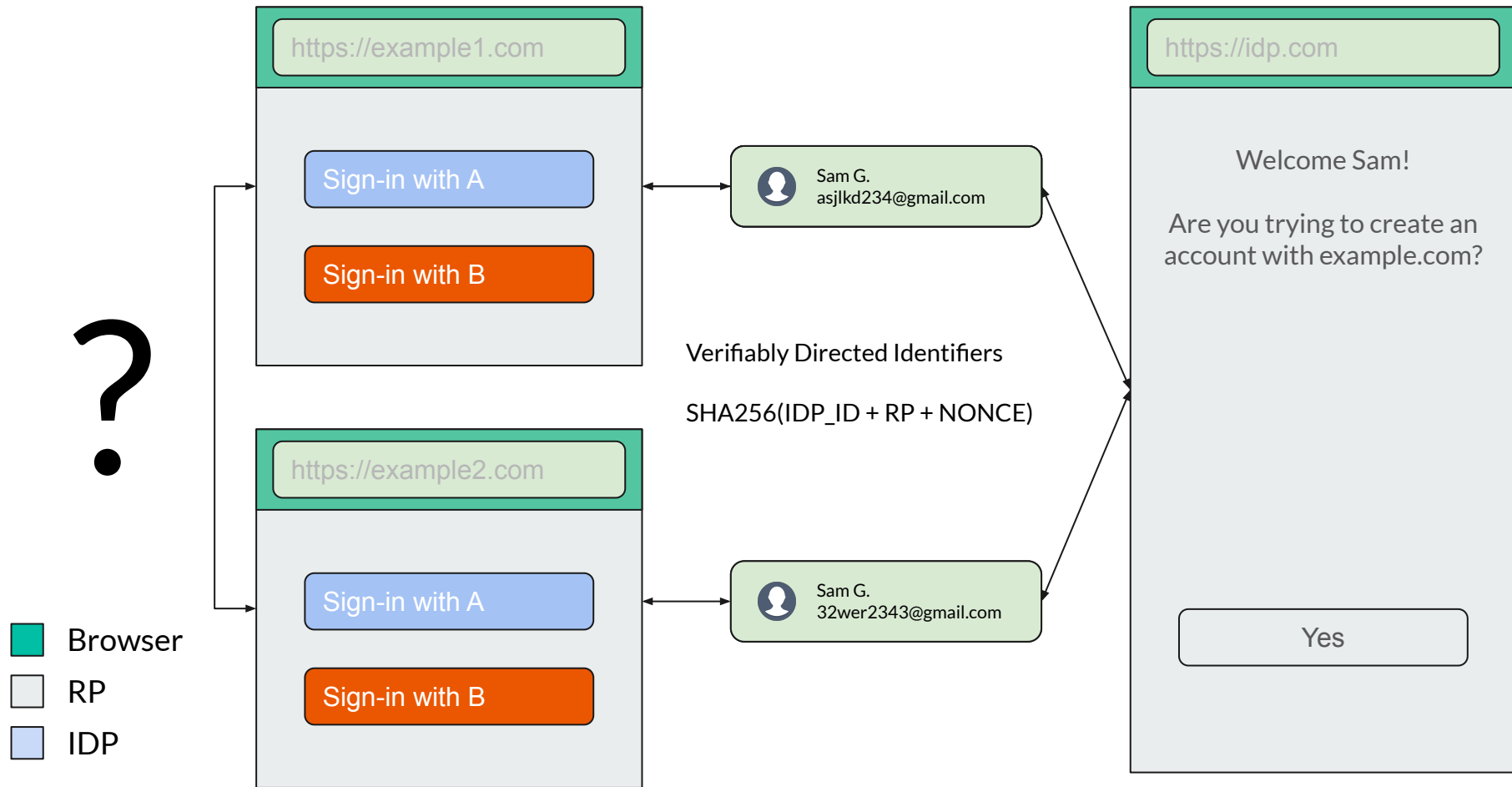
This project is in very early stages and everything below is still considered exploratory.



Complex Trade-offs



Directed Identifiers





Alternatives under consideration

- Approaches for designing a new API fall into three general buckets:
 - The *Permission-oriented* Variation
 - The *Mediation-oriented* Variation
 - The *Delegation-oriented* Variation



UA

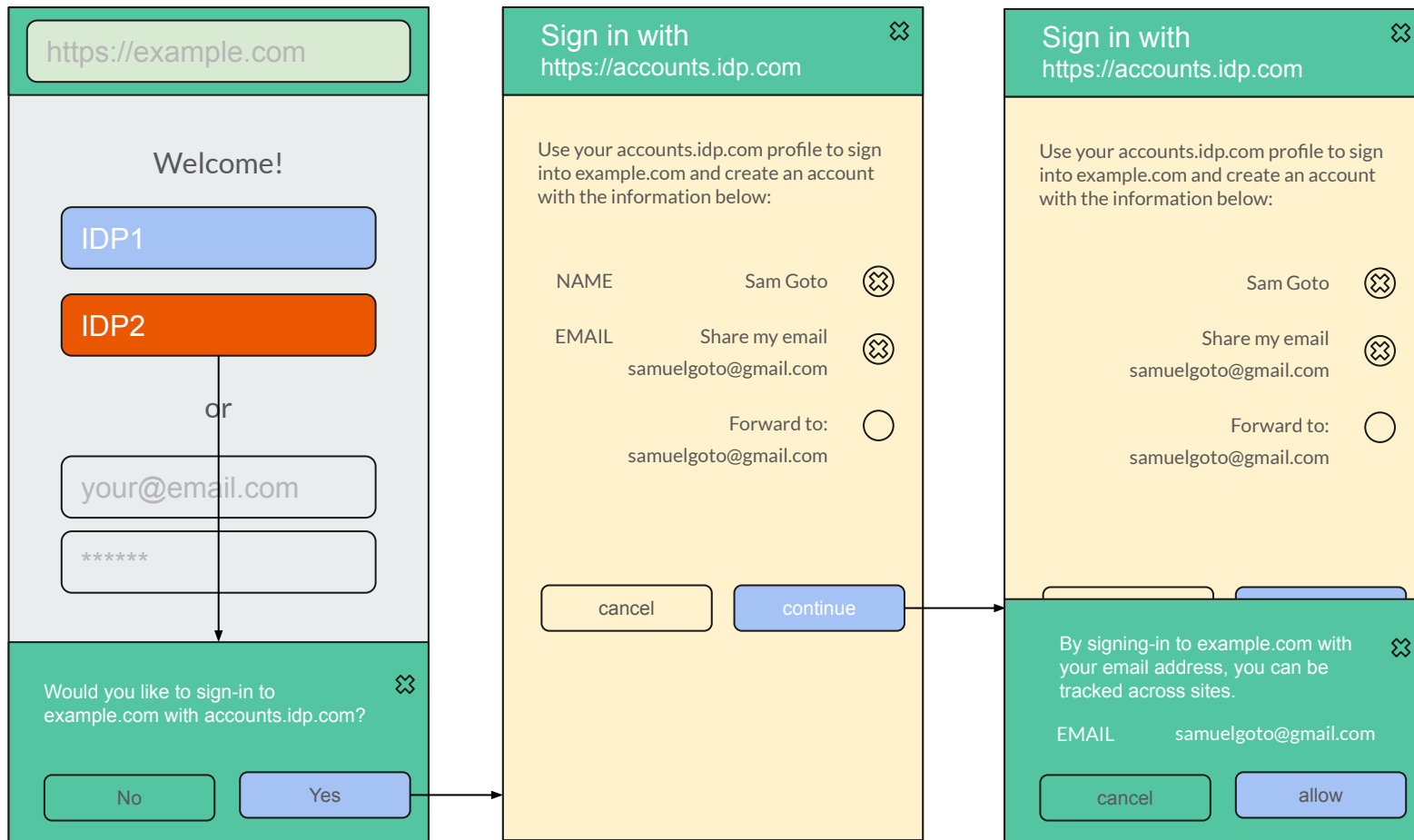


IDP



RP

#1 The Permission-oriented Variation





User Agent



Relying Party

#2 The Mediation-oriented Variation





IDP Tracking

- Neither the permission-based nor mediation-based approach limits the ability of the IDP to know where the user has signed in using the IDP credentials.
- Delegation-based approach redefines the role of an IDP to address that.



User Agent



Email Proxy
(proxy.com)



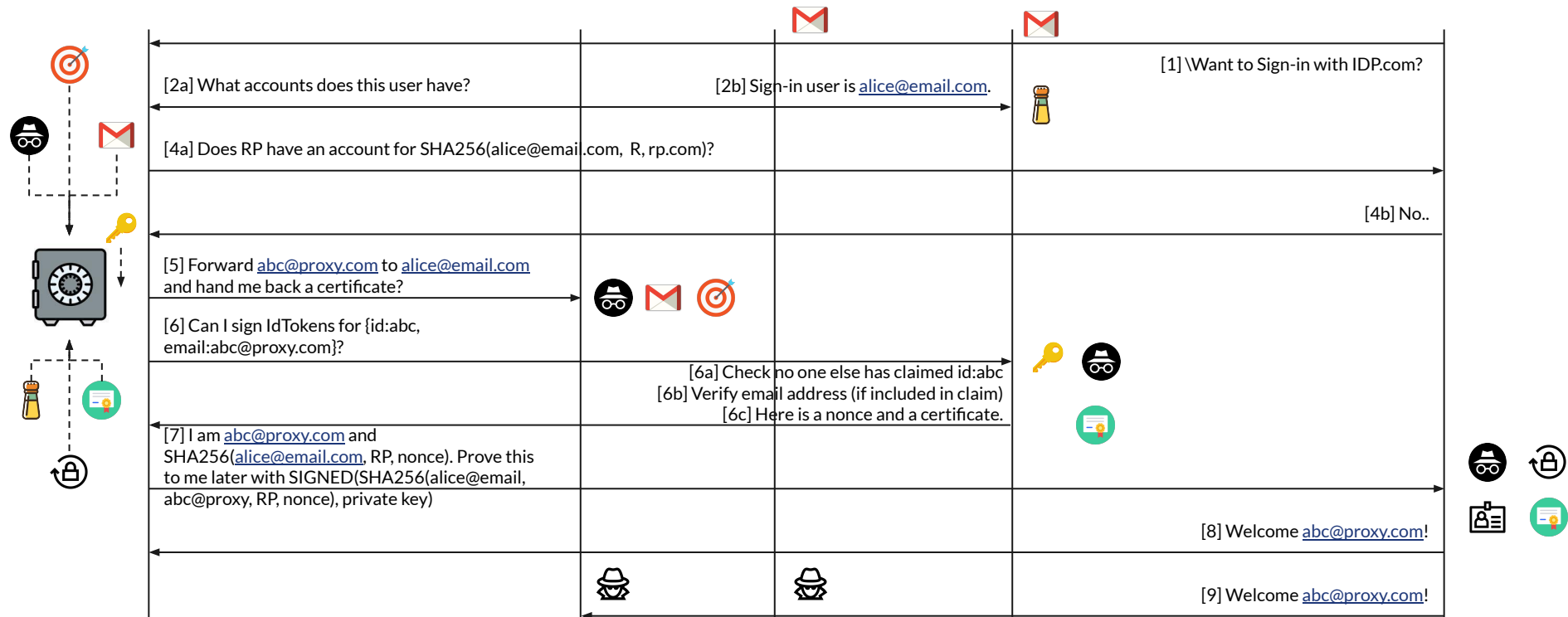
Email Provider
(email.com)



Identity Provider
(idp.com)



Relying Party
(rp.com)



#3 The Delegation-oriented Variation



global email



directed email



keypair



certificate

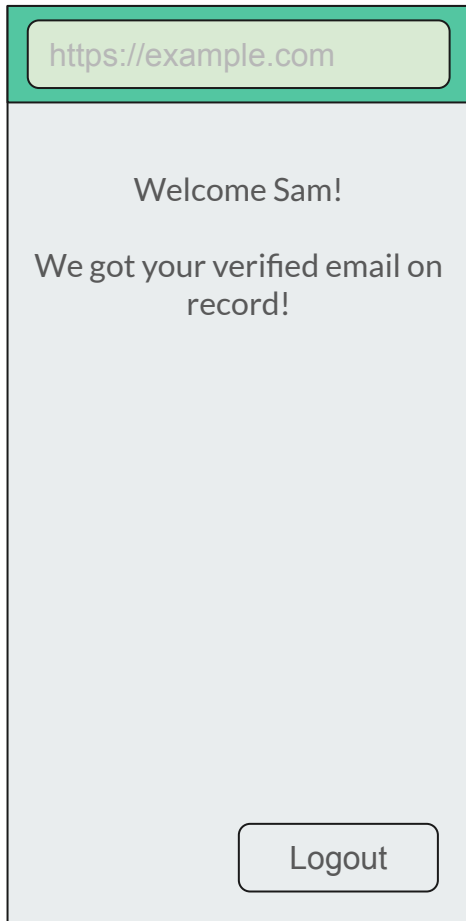


nonce



recovery token

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@email.example",
  "email_verified": "true",
}
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  SECRET
)
```


Aside: 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

Looking Forward



Challenges

- Ecosystem design
 - Can RPs do their job well enough with directed identifiers? Customer support classic example.
- Technical questions
 - To what extent can we programmatically enforce directed identifiers?
 - How valuable are technical enforcement measures over policy requirements for IDP behaviour?
 - What about server-to-server communication that is in common use today?
- Accommodating other use cases
 - Should enterprise policies play a role in setting a different privacy bar for [enterprise SSO](#)? How would we handle “bring your own device” scenarios?



Engagement

- Many stakeholders:
 - RPs
 - IDPs
 - Browsers
 - Other identity ecosystem participants
- Feedback is welcome on <https://github.com/WICG/WebID>

This deck is shared publicly.
