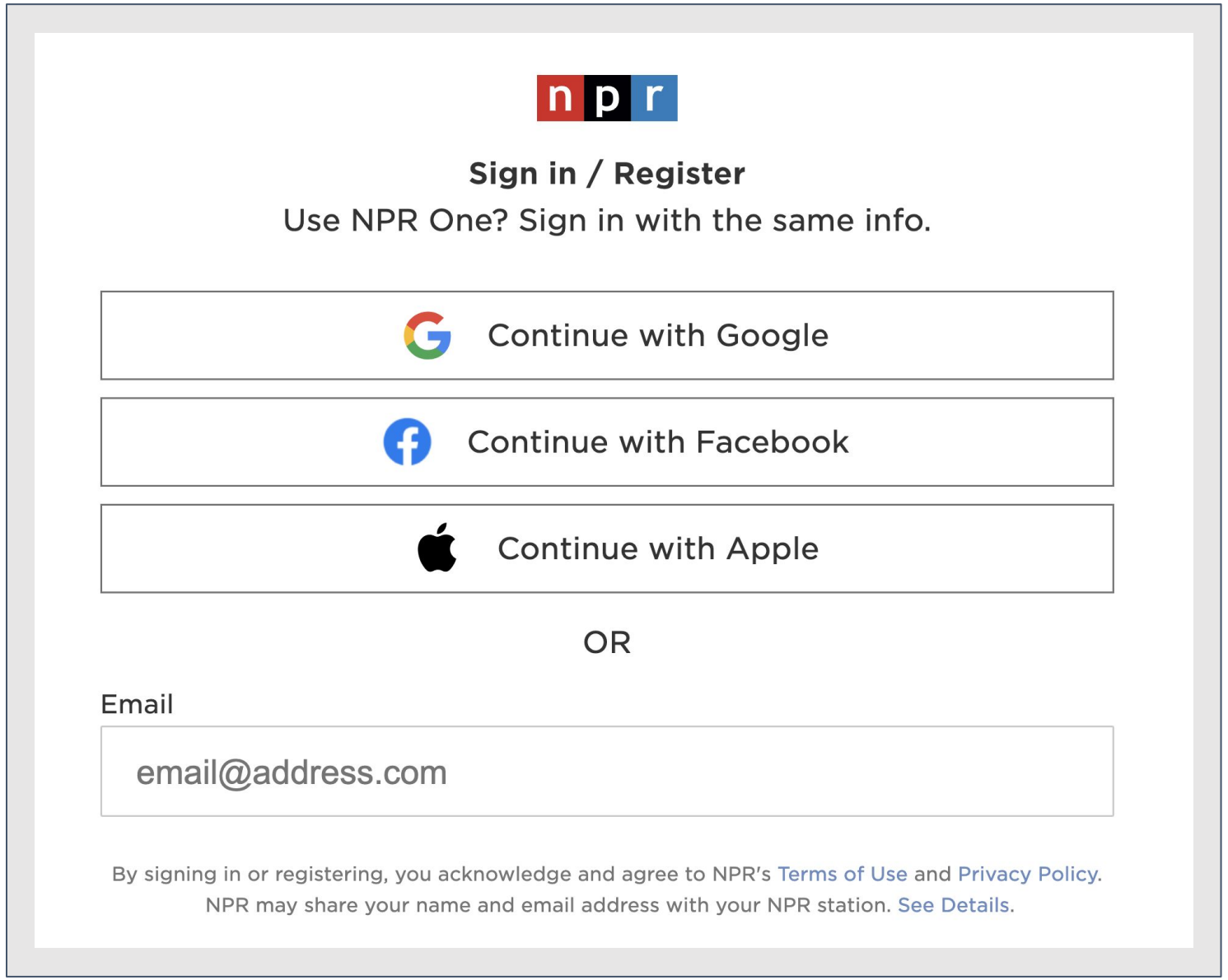
Privacy & Identity Federation

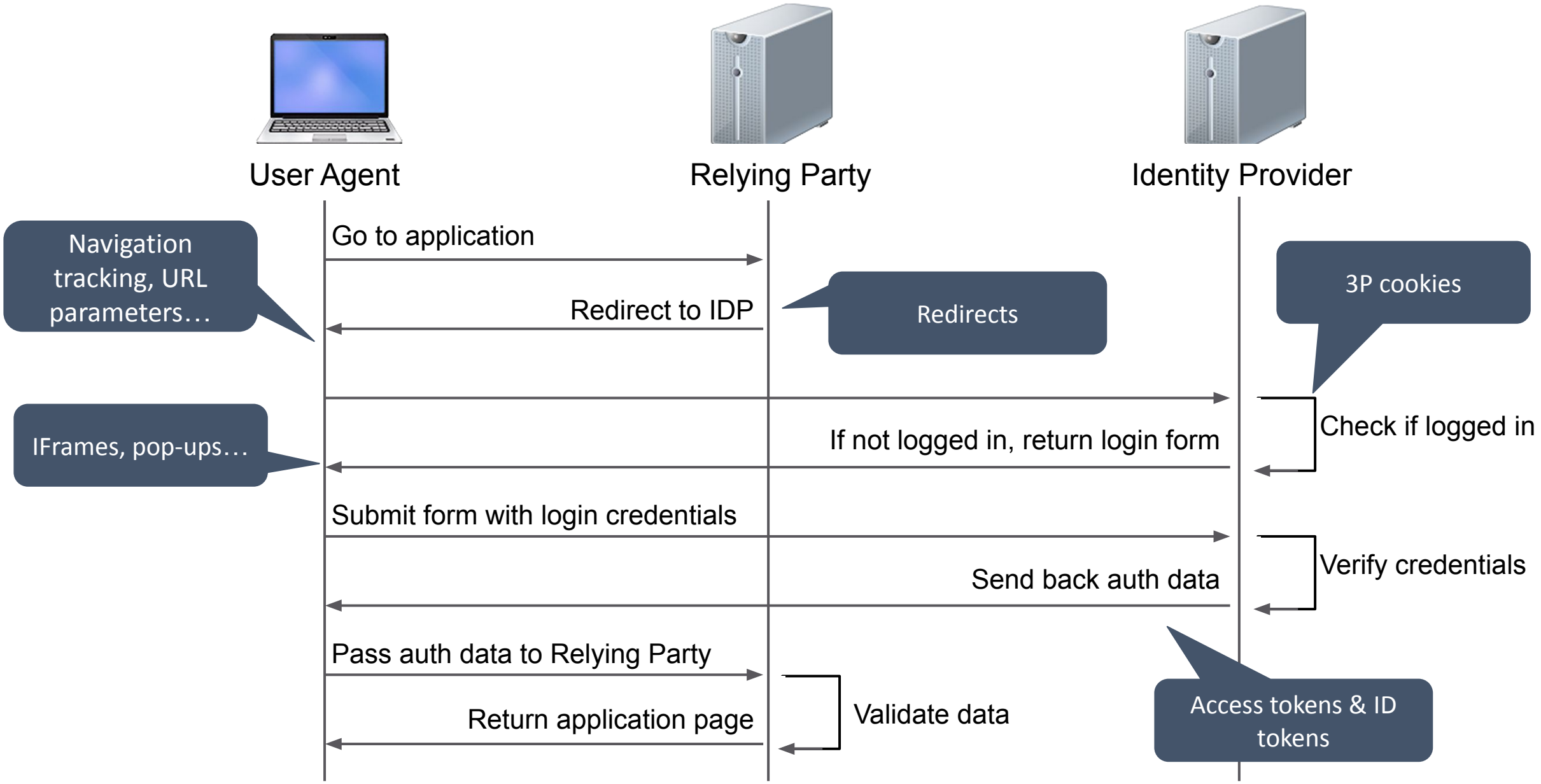
TPAC 2022

Identity Federation



The ability to login to one system using your account from a different system.

Privacy Changes Often Impact Identity Federation



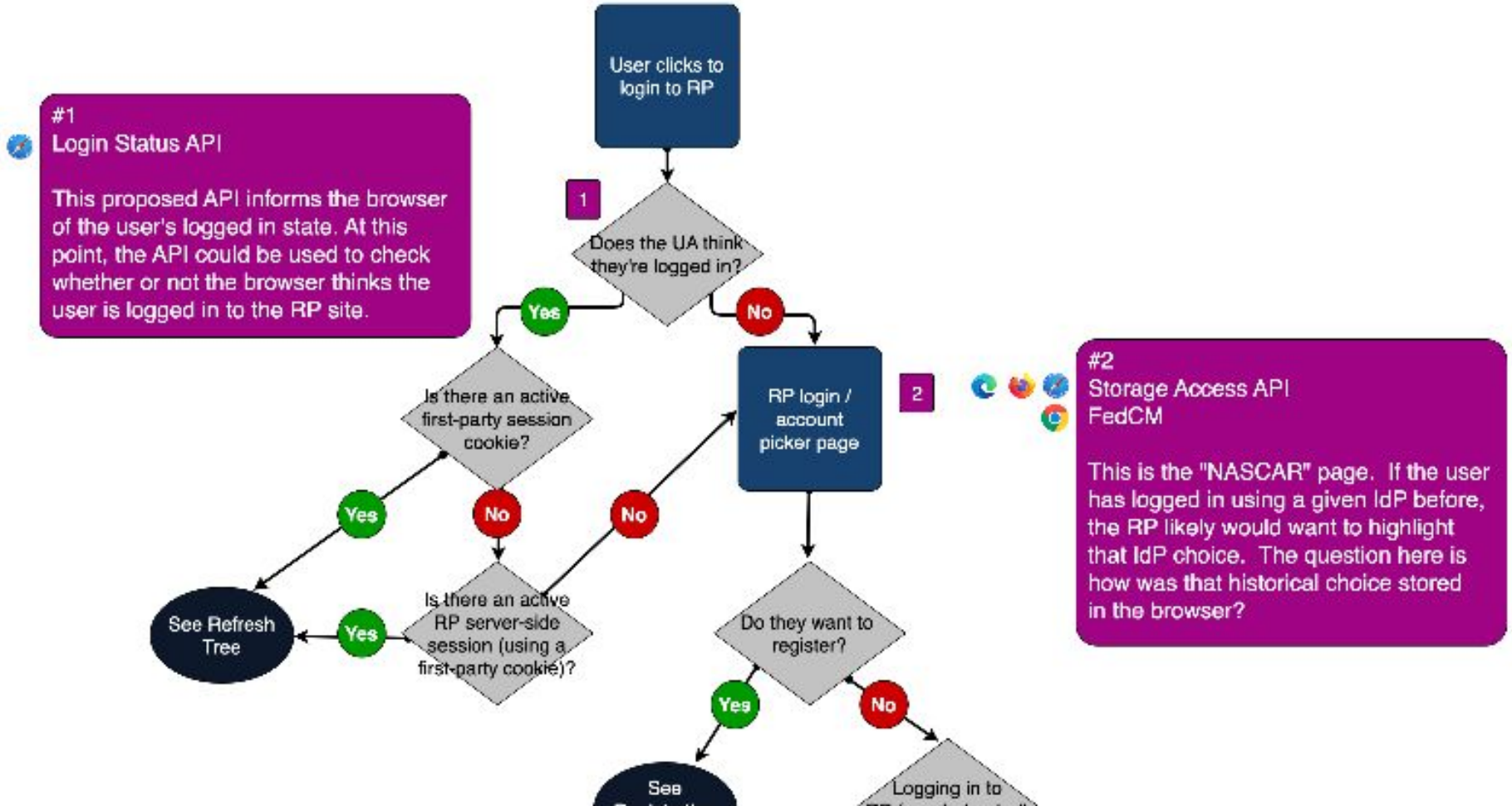
The Challenges

- There aren’t just one or two ways to implement identity federation. Implementations are often unique to the relying parties.
- The organizations that rely on identity federation are not just commercial organizations with dedicated developers. It’s often used in higher education, by governmental agencies, small businesses, etc.
- There aren’t just a handful of identity providers. There are actually thousands which also come from very diverse organizations.

We Created Decision Trees To Identify Options

Federated Login Tree:

OIDC & OAuth 2
Authorization Code Flow
(front-channel & back-channel)



#1
Login Status API

This proposed API informs the browser of the user's logged in state. At this point, the API could be used to check whether or not the browser thinks the user is logged in to the RP site.

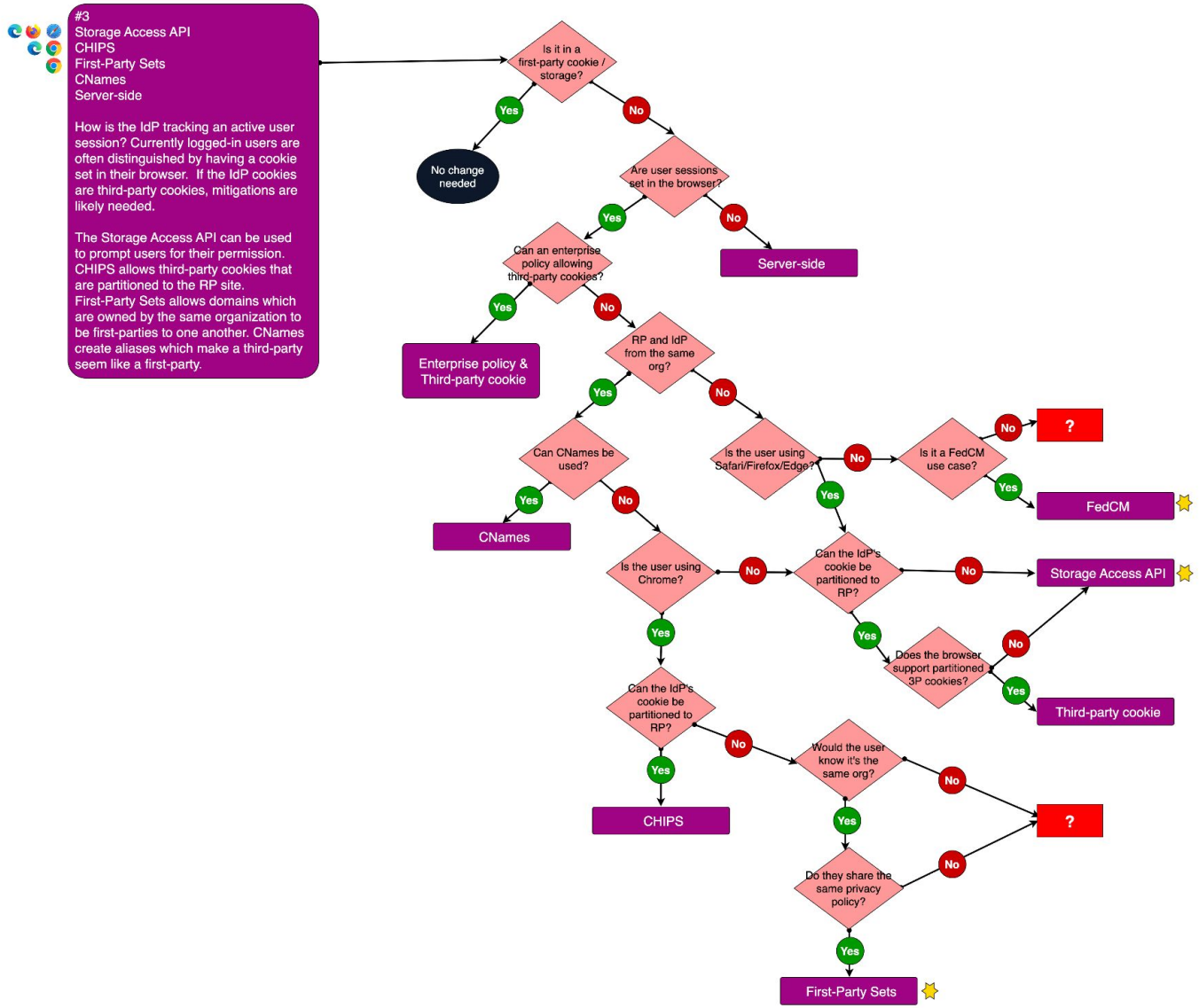
#2
Storage Access API
FedCM

This is the "NASCAR" page. If the user has logged in using a given IdP before, the RP likely would want to highlight that IdP choice. The question here is how was that historical choice stored in the browser?

Proposals That Might Come Into Play

Proposals	
Federated Credentials Management (FedCM)	It supports some identity federation use cases. Focused on the loss of third-party cookies
Storage Access API	Accessing client storage - but there are potential issues
CHIPS	Using partitioned third-party cookies
First-Party Sets (FPS)	When the domains are owned by the same organization
Login Status API (aka isLoggedIn)	A signal for whether the user agent knows if the user is logged in
CNames	Relying parties setting up a CName for the Identity Provider
Enterprise Policies & Third-Party Cookies	Have enterprises create a policy which allows the use of third-party cookies

If The User Needs To Login



Our Goals/Asks

- We can’t break identity federation
- Proposals are developed for where there aren’t identified solutions for
- Proposals take into consideration the federated identity use cases
- Proposal authors coordinate on how these use cases are handled
- Browser vendors create the decision trees they expect developers to use for their browser
- The more unified these trees are across browsers, the better!

User Session Management