Signing Out and Session Management in 2023

Vittorio Bertocci

Principal Architect

OKTA

@vibronet

Safe harbor

This presentation contains “forward-looking statements” within the meaning of the “safe harbor” provisions of the Private Securities Litigation Reform Act of 1995, including but not limited to, statements regarding our financial outlook, long-term financial targets, product development, business strategy and plans, market trends and market size, opportunities, positioning and expected benefits that will be derived from the acquisition of Auth0, Inc. These forward-looking statements are based on current expectations, estimates, forecasts and projections. Words such as “expect,” “anticipate,” “should,” “believe,” “hope,” “target,” “project,” “goals,” “estimate,” “potential,” “predict,” “may,” “will,” “might,” “could,” “intend,” “shall” and variations of these terms and similar expressions are intended to identify these forward-looking statements, although not all forward-looking statements contain these identifying words. Forward-looking statements are subject to a number of risks and uncertainties, many of which involve factors or circumstances that are beyond our control. For example, the market for our products may develop more slowly than expected or than it has in the past; our results of operations may fluctuate more than expected; there may be significant fluctuations in our results of operations and cash flows related to our revenue recognition or otherwise; the impact of COVID-19 and variants of concern, related public health measures and any associated economic downturn on our business and results of operations may be more than we expect; a network or data security incident that allows unauthorized access to our network or data or our customers’ data could damage our reputation; we could experience interruptions or performance problems associated with our technology, including a service outage; we may not be able to pay off our convertible senior notes when due; we may fail to successfully integrate any new business, including Auth0, Inc.; we may fail to realize anticipated benefits of any combined operations with Auth0, Inc.; we may experience unanticipated costs of integrating Auth0, Inc.; the potential impact of the acquisition on relationships with third parties, including employees, customers, partners and competitors; we may be unable to retain key personnel; and global economic conditions could deteriorate. Further information on potential factors that could affect our financial results is included in our most recent Quarterly Report on Form 10-Q and our other filings with the Securities and Exchange Commission. The forward-looking statements included in this presentation represent our views only as of the date of this presentation and we assume no obligation and do not intend to update these forward-looking statements.

Any unreleased products, features or functionality referenced in this presentation are not currently available and may not be delivered on time or at all. Product roadmaps do not represent a commitment, obligation or promise to deliver any product, feature or functionality, and you should not rely on them to make your purchase decisions.

okta

Agenda

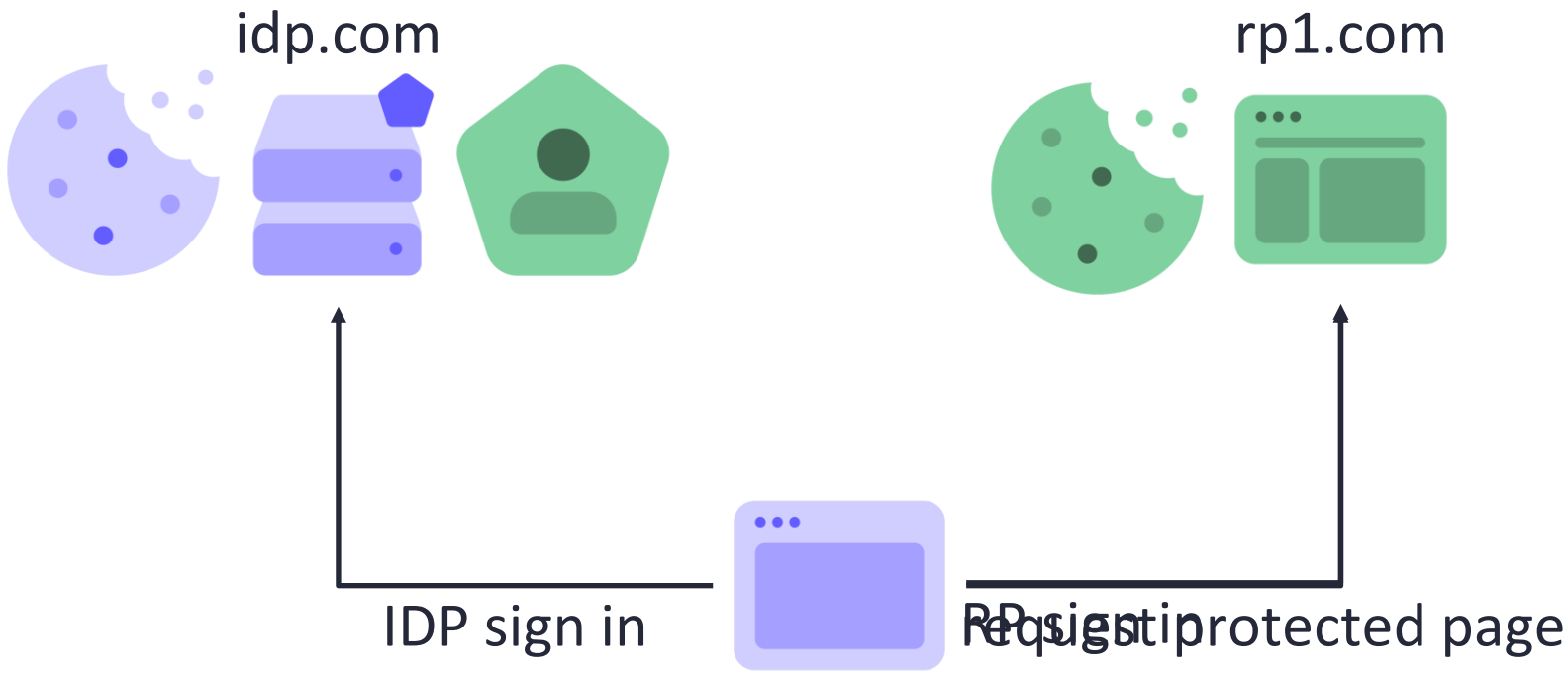
- What does “sign out” even mean?
- Traditional sign out techniques and the 3PC threat
- Modern sign out and session management
- Looking ahead

What does “sign out” even mean?

Definitions

- **Session**
  a time interval during which a user/app can access a resource without being prompted
  - Also: the artifact(s) that make that behavior possible

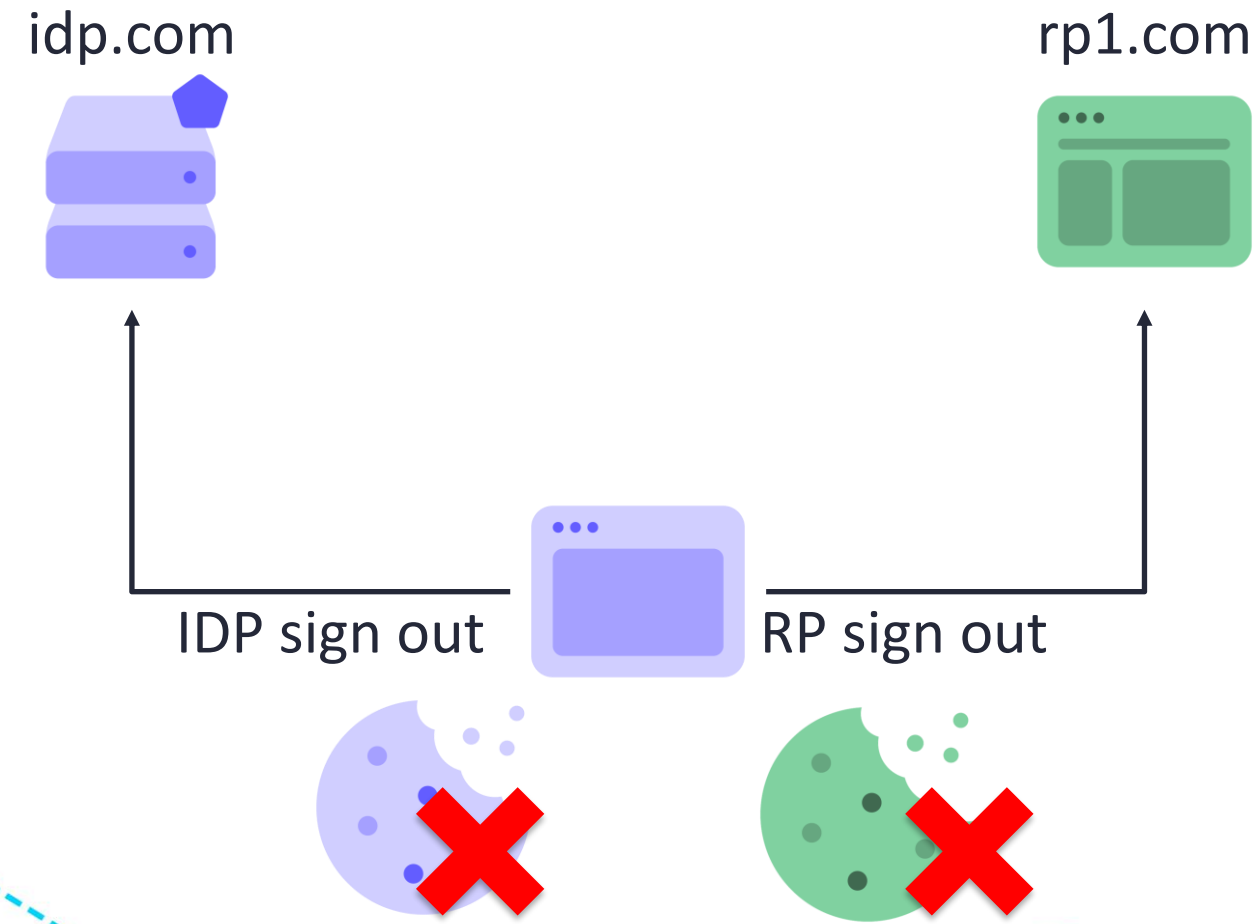
Signing In



Definitions

- **Session**
  a time interval during which a user/app can access a resource without being prompted
  - Also: the artifact(s) that make that behavior possible
- **Sign Out**
  the act of terminating a session for an app (and the IdP's session that created it, if any)

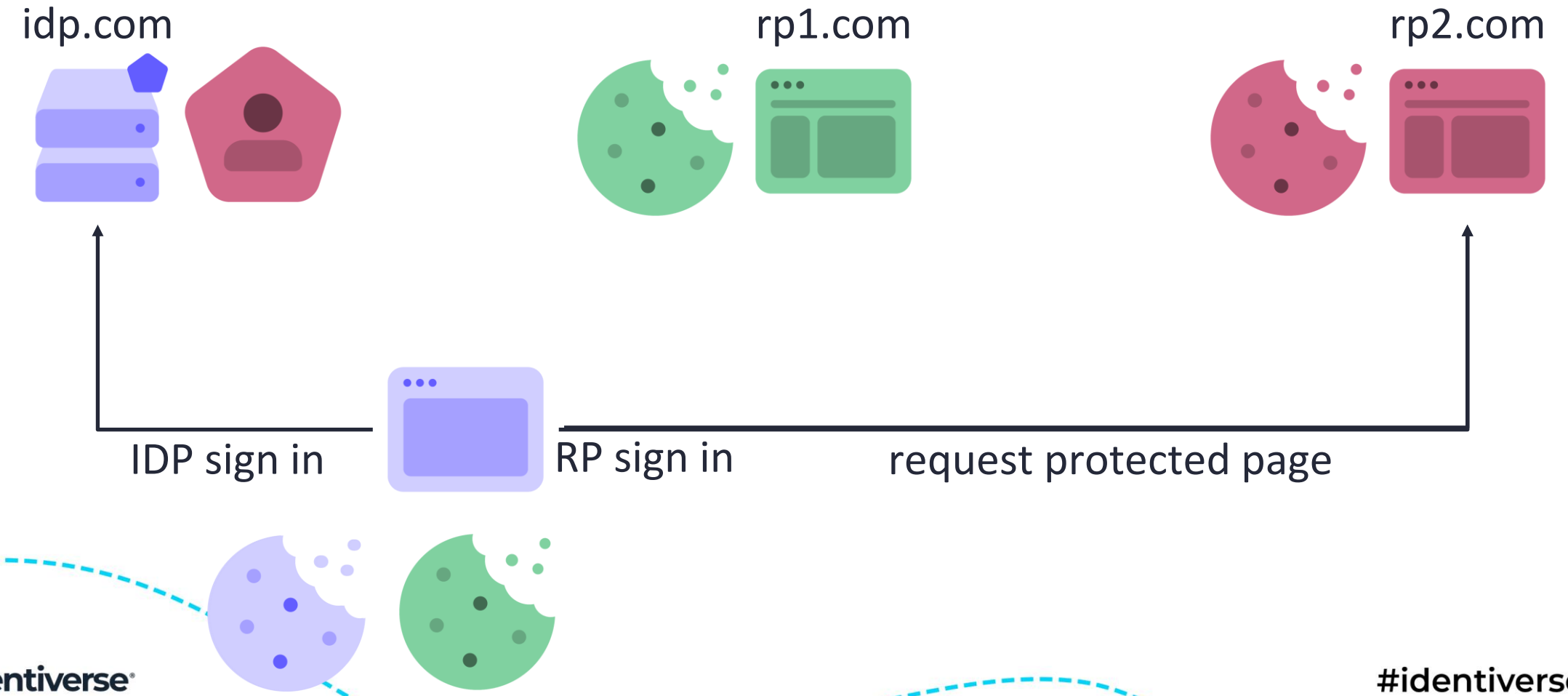
Signing Out



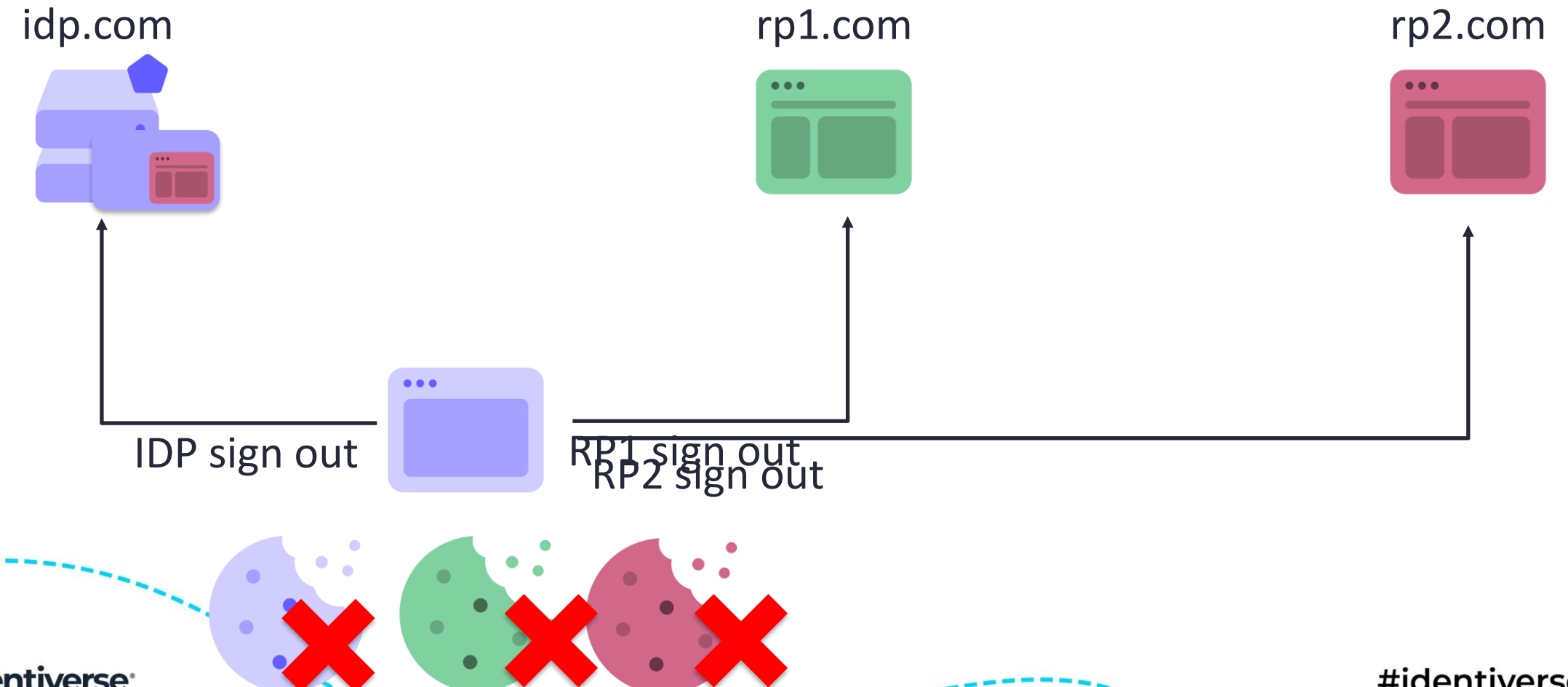
Definitions

- **Session**
  a time interval during which a user/app can access a resource without being prompted
  - Also: the artifact(s) that make that behavior possible
- **Sign Out**
  the act of terminating a session for an app (and the IdP's session that created it, if any)
- **Distributed Sign Out** (or Single Log Out, SLO)
  Sign Out + the act of signing out from all the apps whose sessions have been created from the same IdP session

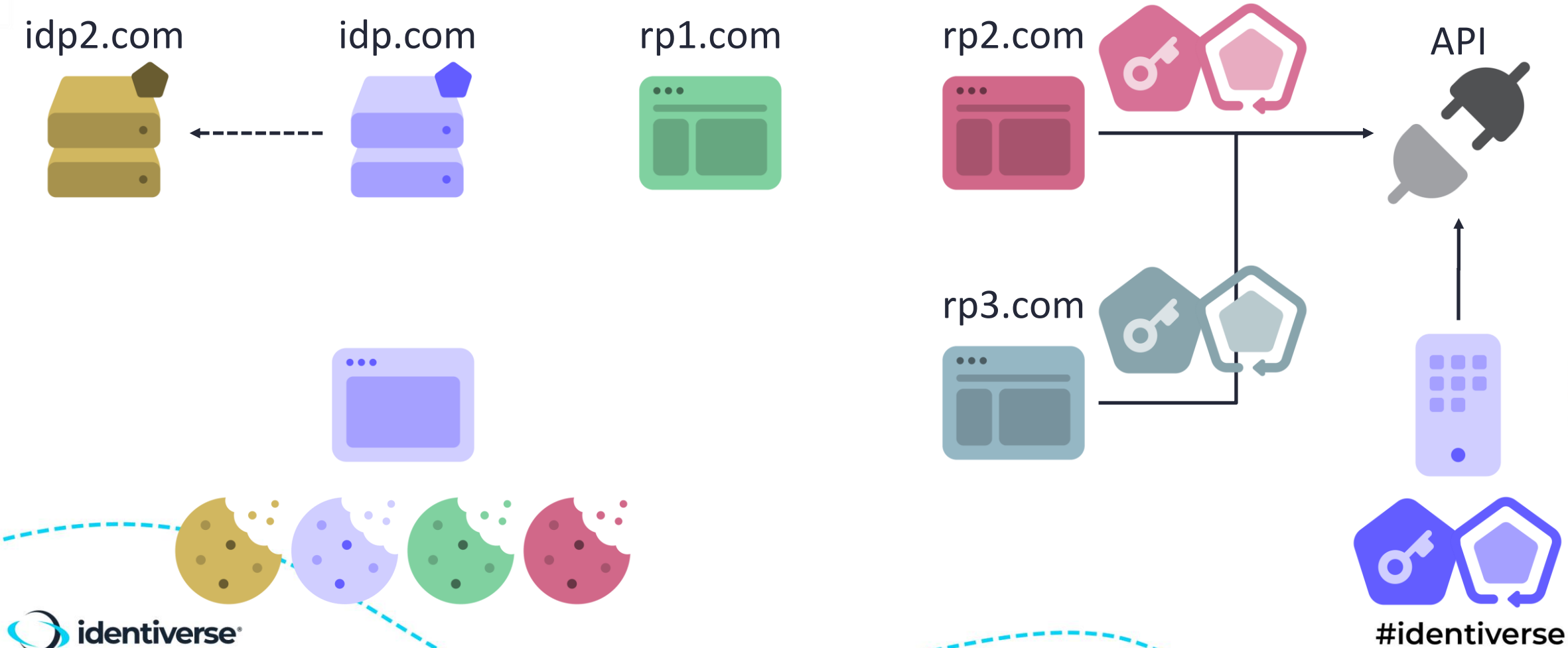
Single Sign On



Distributed Sign Out



Today Things are More Complicated

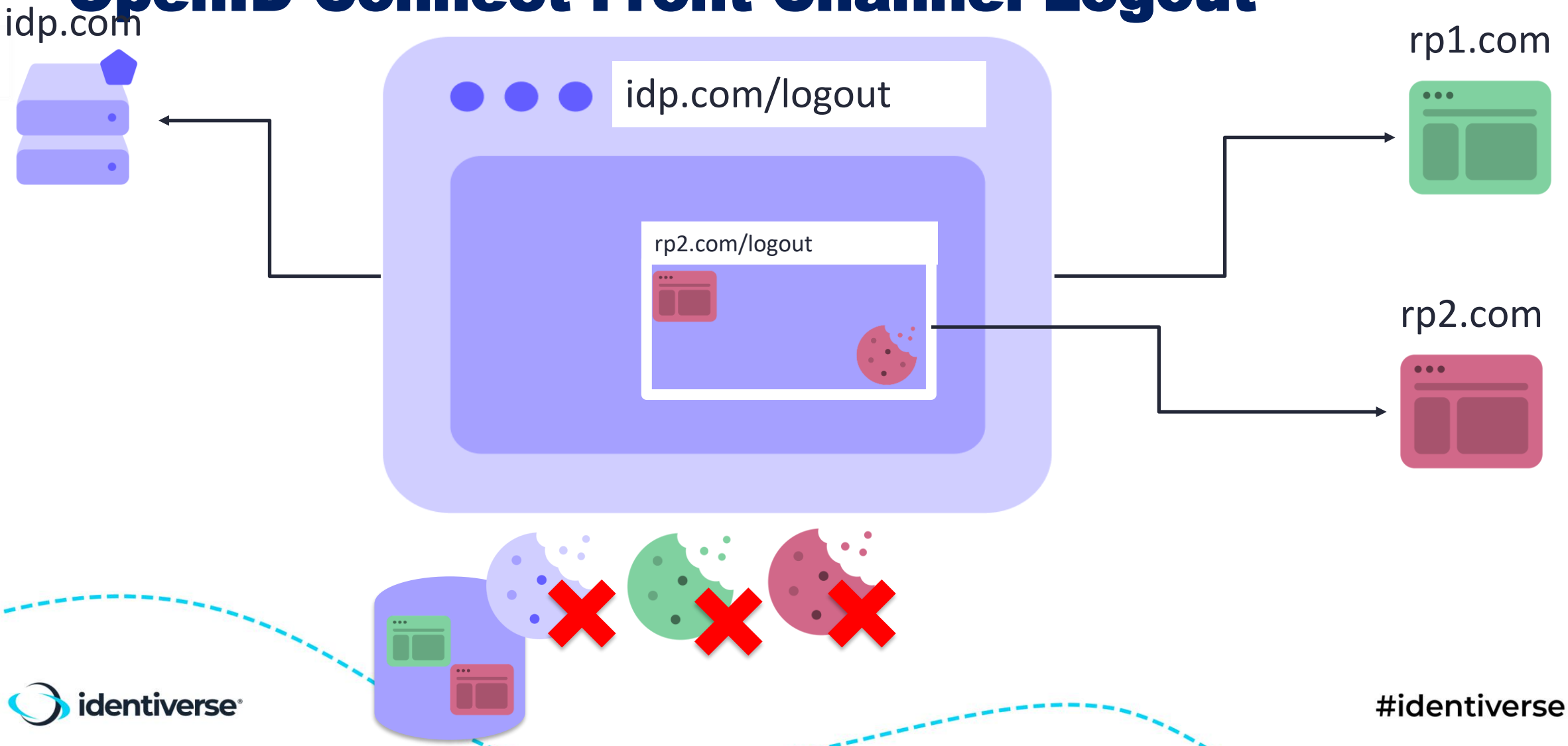


Traditional Sign Out Flows

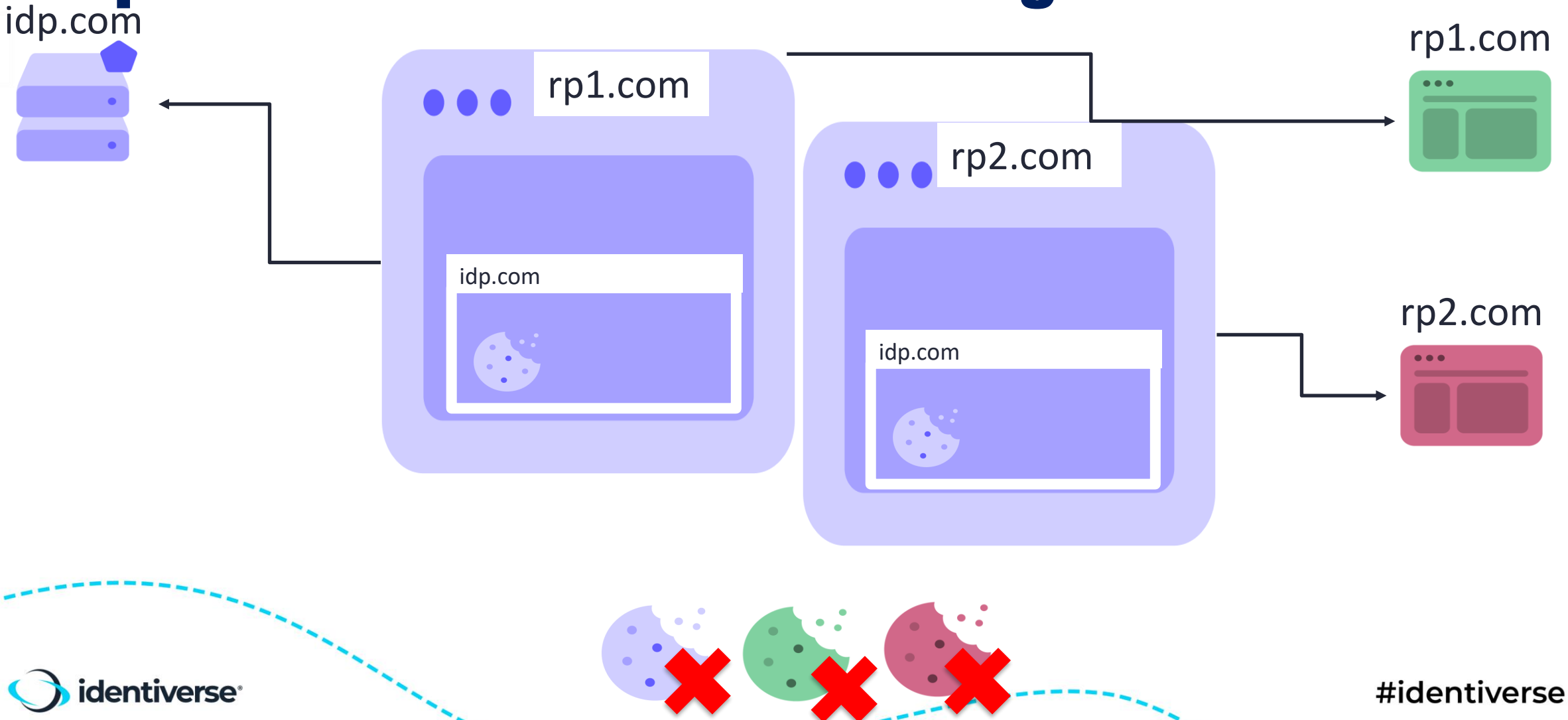
Web SLO Flows In Use Today

- OpenID Connect
  - Front channel logout
  - Session management
- SAML

OpenID Connect Front Channel Logout



OpenID Connect Session Management



What About SPAs and Native Apps?

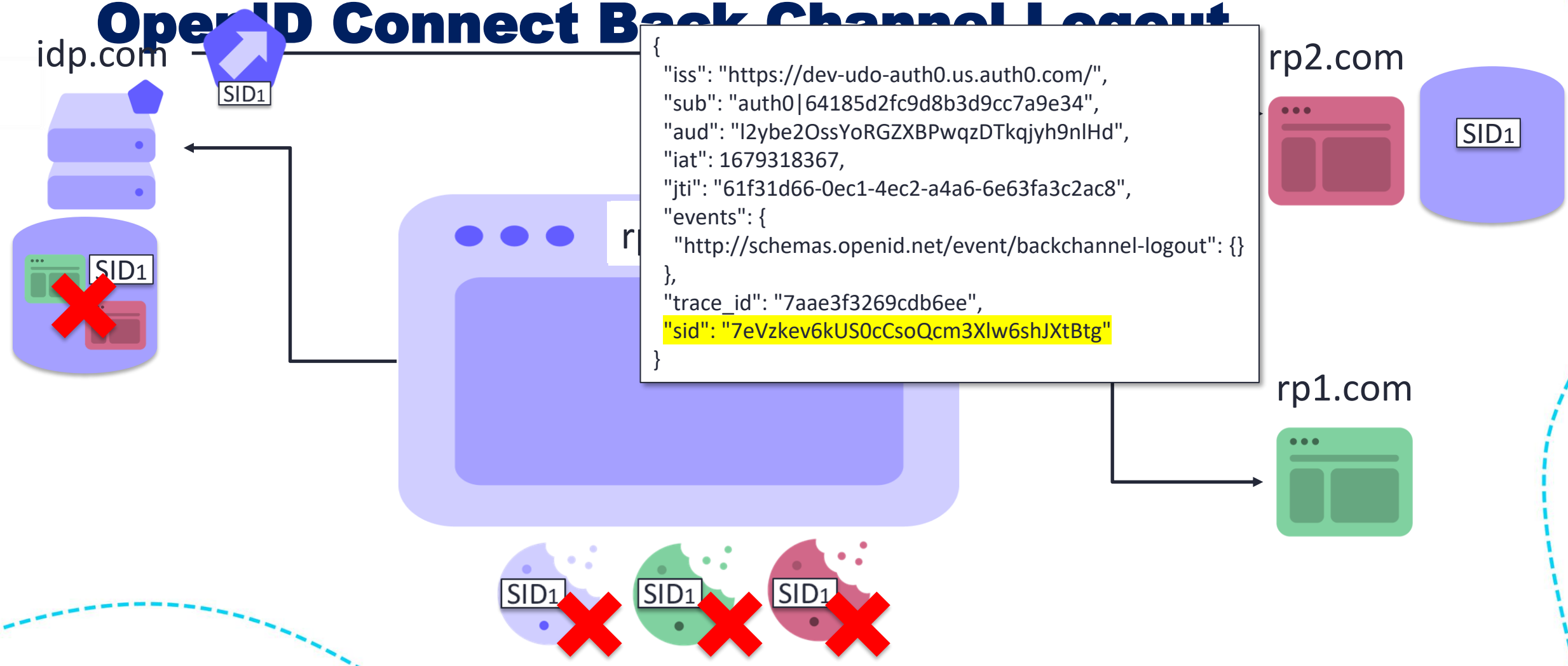
- With 3PC deprecation, OIDC session management will stop working
  - And it wouldn't help with mobile apps anyway
- No standard way to tie access/refresh token lifetimes to session's
- Emergent (but still blurry standards) for control plane

Modern Approaches to Sign Out

Assorted Tricks to Preserve Traditional SLO Flows

- Using CNAME to put Idp and ONE RP on the same domain
- First Party Sets
- Etc

OpenID Connect Back Channel Logout



SSF/CAEP?

- Shared Signal Framework in OpenID Foundation
- Mechanism to distribute events
  - Used by Continuous Access Evaluation (CAEP) and Risk Incident Sharing and Coordination (RISC)
- Could be used to send sign out signals

Looking Ahead

Looking Ahead

- The deprecation of 3rd party cookies WILL force action
- Apps will need to move to 3PC-free SLO methods
- We need a control plane for non-web apps, persistent sessions
- Watch this space

No Time to Lose!

- Next week:
  - Identify what shapes “session” takes within your organization
- In three months:
  - Identify what protocols are in use, and what requirements current deployments have
  - Experiment with modern sign out approaches on small pilots
- Within six months:
  - Start migrating the solutions at most imminent risk of disruption
  - Have a complete plan for rationalizing and future-proofing session management company wide

- @vibronet

Grazie Mille

- @vibronet