Identity vs Browser Changes

Tim Cappalli | Vittorio Bertocci

Agenda

- Blast Radius
- Use Cases
- Current Proposals
- Discussion!

Blast Radius

- Third-Party Cookies
- Link Decoration
- Bounce Tracking
- Identity-specific APIs
- Browser assuming active role in identity flows

Sign In and Sign Out

Usage	Protocol	Flow	3P Cookies	Link Decoration	Redirect
Sign-in	OIDC	Implicit + form POST	No	Yes	Yes
Sign-in	OIDC	Code flow	No	Yes	Yes
Sign-in	OIDC	SPA: Code + PKCE	No	Yes	Yes
Sign-in	OIDC	SPA: Implicit, fragment	No	Yes	Yes
Sign-in	SAML 2.0	Redirect + POST	No	Yes	Yes
Sign-in	SAML 2.0	Artifact binding	No	Yes	Yes
Sign-in	WS-Federation	Redirect + POST	No	Yes	Yes
Sign-out	OIDC	RP-Initiated Logout	No	Yes	Yes
Sign-out	OIDC	Front-Channel Logout	**Yes**	Yes	No
Sign-out	OIDC	Session Management	**Yes**	No	No
Sign-out	SAML 2.0	Single Log Out (SLO)	**Maybe**	Yes	Yes

Access and Refresh Tokens

Usage	Protocol	Flow	3P Cookies	Link Decoration	Redirect
Token Retrieval	OAuth 2.0	Code flow	No	Yes	Yes
Token Retrieval	OAuth 2.0	SPA: Code + PKCE	No	Yes	Yes
Token Renewal	OAuth 2.0	SPA: background token renewal (iframe)	**Yes**	Yes	Yes
Token Renewal	OAuth 2.0	SPA: background token renewal (refresh token)	No	No	No
Token Usage	OAuth 2.0	JS bearer token	No	No	No

Current Proposals

- Login Status API (formerly IsLoggedIn)
- Storage Access API
- First Party Sets
- Cookies Having Independent Partitioned State (CHIPS)
- Federated Credential Management (formerly WebID)

Current Proposals

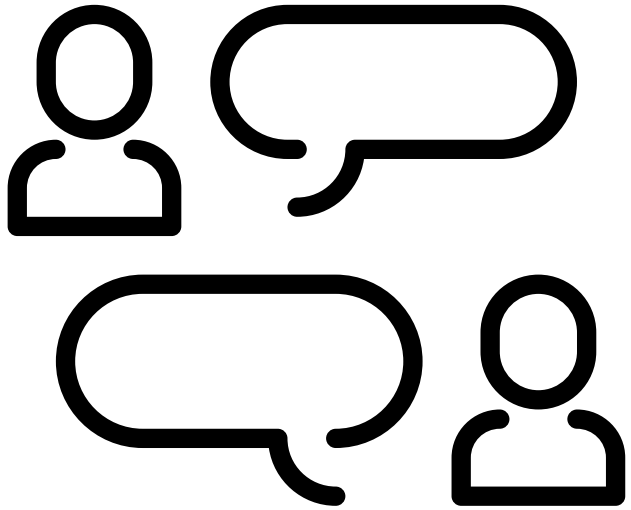
Proposal Name	What it does…	What is helps with…
Login Status API (Privacy CG)	websites can inform the web browser of the user's login status	Could be used as a signal for browser tracking protection logic
Storage Access API (SAA) (Privacy CG)	enable content in iframes to request access to website data (such as cookies)	Grant access to cookies and other local artifacts in iframes
First Party Sets (FPS) (Privacy CG)	Allow related domain names to declare themselves as the same first-party	Preserves 3P cookies across domains with a mutually agreed upon relationship
Cookies Having Independent Partitioned State (CHIPS) (Privacy CG)	Servers can indicate they'd wish to set a cross-site cookie which is partitioned by top-level site	Allows embedded frames to continue using 3P cookies without a tracking vector
Federated Credential Management (FedCM) (Currently WICG)	User agent mediation of identity flows	Cookie access for iframes and XHR/fetch requests

Call to Action

https://www.w3.org/community/fed-id/

- Join the Federated Identity Community Group!
- Help us document use cases and protocol flows
- Impact analysis of proposed browser changes against your deployed solutions

- If you think you have a unique but compelling use case for the use of 3P cookies in auth flows, but cannot join the CG, please contact Heather Flanagan (hlf@sphericalcowconsulting.com)



Discussion!

https://github.com/privacycg/is-logged-in

Login Status API

Goals

- websites can inform the web browser of the user's login status

Methods

- `navigator.recordLogin(); navigator.recordLogout(); navigator.checkLoginState();`
- potential tie in with WebAuthn and password managers for abuse mitigations

Status

- Explainer

https://privacycg.github.io/storage-access/

Storage Access API (SAA)

Goals

- enable content in iframes to request access to website data (such as cookies)

Methods

- `requestStorageAccess();`

Status

- Chrome: Opposed | Edge: In Dev | Safari: Shipped | Firefox: Shipped
- W3C Privacy CG Work Item

https://privacycg.github.io/first-party-sets/

First Party Sets (FPS)

Goals

- Allow related domain names to declare themselves as the same first-party (ex: office.com, sharepoint.com, dynamics.com, login.microsoftonline.com)

Methods

- .well-known URL
- Static UA-provided list
- Static user-managed list
- Static admin policy list

Status

- Chrome: Post-OT Review | Edge: Post-OT Review | Safari: *mixed* | Firefox: "Harmful"
- TAG review

https://github.com/WICG/CHIPS

Cookies Having Independent Partitioned State (CHIPS)

Goals

- Binds cookies from embedded frames to the parent frame origin

Methods

- Cookies must be set with a new attribute in order to be sent on cross-party requests once (unpartitioned) third-party cookies are obsoleted
- partition-key = top-level site or FPS owner
- `Set-Cookie: __Host-SID=31d4d96e40; SameSite=None; Secure; HttpOnly; Path=/; Partitioned;`

Status

- W3C WICG Proposal

https://wicg.github.io/FedCM/

Federated Credential Management (FCM)

Goals

- address flows broken by 3P cookie deprecation in iframes and XHR/fetch requests

Methods

- User agent mediates authentication flows

Status

- WICG explainer and draft