Federated Identity Community Group

28 July 2021

Agenda

- Background and Problem Statement
- About Tracking
- Timing and Browser Development Activities
- W3C’s FedID CG

Background

- As browsers take steps to support user privacy, they are deprecating certain features such as third-party cookies, bounce tracking, link decoration, and so on.
- Many of these features are also used by federated identity protocols.

The Short, Short Version

- Authentication that uses SAML will continue to work as designed for at least the next 2-3 years (excepting the ability to globally log out of all SAML sessions).
- Authentication that uses OIDC is already starting to break.
- Services (like SeamlessAccess) that use browser local storage so that many domains can read the same data are going to have to have mixed results.

General Problem Statement

Non-transparent, uncontrollable tracking of users across the web needs to be addressed and prevented.

We have rough consensus on this as a place to start as of the Federation and Browser Workshop held 25-26 May 2021.

Federated Identity Addendum

Applications and services need to work through browser to support SSO/federated login, and yet federated login and tracking tools use the same primitives and are indistinguishable from the browser’s perspective.

How Does Tracking Happen?

- Third-Party Cookies
- Bounce Tracking
- IP Addresses
- Browser Fingerprinting
- Link Decoration

What’s Changing in the Next 2-3 Years?

Features that Can Be Used for Tracking

- If it can be used for tracking, it is under consideration for a major redesign
- Third-party cookies are top of the list of things to be removed in favor of a more privacy-preserving default web experience

Going on a Diet

Safari: third-party cookies are **already** blocked by **default**

Firefox: third-party cookies are **already** blocked **by a blocklist**, and

Chrome (desktop): “phase out third-party cookies over a three month period, starting in mid-2023 and ending in late 2023”

What Breaks When Third-Party Cookies are Gone

SAML Single Log Out will break (depending on how a vendor has implemented it)

Several OIDC/OAuth2 features will break (e.g., front-channel logout, session management, iFrame-based session extension, SPA background token renewal)

IdP persistence will break because of the third-party nature of the information (e.g., IdP discovery services, SeamlessAccess)

Cookies and Federation Behavior

- If you want to emulate the worse case of how the lack of cookies will impact software in use, test with Safari
  - Example: Microsoft Teams won't work in Safari
- If you want to emulate how Chrome (desktop) breaks, change your config to reject all third-party cookies, with a couple of special notes:
  - First-Party Sets / SameParty cookies will be exempt (https://github.com/cfredric/sameparty)
  - Partitioned cookies and storage will be exempt

So many conversations, so little time

- Several orgs are grappling with different perspectives on the problem
  - IETF / OAuth2.0 WG
  - OIDF's Browser Interaction special interest group (closing as of 28 July 2021)
  - W3C's WICG, PrivacyCG, FedID CG, Web Advertising Business Group, …
  - InCommon Technical Advisory Committee, REFEDS

The Federated Identity Community Group

- In scope:
  - Prototyping changes to the federated authentication workflow to mitigate tracking possibilities.
    - Specifically, user agent features and APIs
- Out of Scope (short-term)
  - Design around identity-related scenarios which are not applicable to federated identity flows impacted by upcoming privacy-preserving platform changes. For example, fully-decentralized topologies.
  - Ad-tech tools or APIs

Charter, Readme, etc: https://github.com/w3c/fedidcg/