State of browser privacy evolution

Overview

FedCM

FedCM is one of three APIs that appear to have broad support among the three browser engine teams. Broad support means that it's likely all three will eventually support the standard, not that it is implemented. FedCM was released in Chrome in November 2022, and is also implemented in Edge and Opera (built on the Chrome engine). Firefox has a FedCM project tracker in bugzilla indicating active work. Apple stated in the Webkit developer making list that they are generally supportive.
The specification from the W3C FedId community group is under active development. That community group is working on proposing a W3C working group, which has greater authority; at this point, it is in negotiation where the spec will continue development.

Documentation from browser developers can be found for Chrome and Mozilla. See State of FedCM and SAML for more in depth discussion.

### Privacy initiatives

<table>
<thead>
<tr>
<th>How does it work</th>
<th>Mitigations</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Navigational tracking</strong></td>
<td>Safari: Intelligent Tracking Prevention – W3C Privacy CG draft, additional protections when private browsing in Safari 17 – announcement at WWDCE23 Firex desktop: Enhanced Tracking Protection – Mozilla and W3 C Privacy CG draft Proposal Draft: when a user has no interaction with a site (at eTLD+1 level), limit cookies to an hour lifetime.</td>
<td>Authentication protocols use cross-site redirection with &quot;link decoration&quot; and POST to exchange information about the sites and the user. While SSO is understood as a critical element, it is understood much more as a single bounce, consumer side authentication, without the many bounces to translate across protocols and implementations, nor is there understanding the trust models and authorization elements involved. This is the main focus of REFEDS Working group interaction with the W3C groups.</td>
</tr>
<tr>
<td><strong>Third party cookies</strong></td>
<td><strong>Storage Access API or Shared Storage API</strong> allows a site to ask a user to allow third party cookies for that site’s use – documentation from Mozilla. Implemented in Firefox, with caveats in Chrome, Edge, Safari <strong>FedCM</strong>: a new way for an authentication token to be exchanged – see above **Cookies Having Independent Partitioned State (CHIPS, also know as Partitioned cookies) allows an iframe to set cookies that the iframe can retrieve across a specific top level site, but no other site – documentation from Mozilla and Chrome</td>
<td>Third party cookies are not needed at any protocol specification. However, some consumer authentication libraries embedded in various sites and apps use third party cookies. Within SAML, identity federation, and higher ed, implementations of logout (Why are third party cookies relevant to single logout) and of Seamless Access are affected. In Seamless Access, the &quot;smart button&quot; is not available without third party cookies and introduces additional clicks in the flow for sites using advanced integration.</td>
</tr>
<tr>
<td><strong>Cross site request cookies (2021)</strong></td>
<td>Cookies received by a site when a user is directed to that site via a link from another site. In a proposal shared in the W3C WebAppSec WG regarding &quot;Standardizing Security Semantics of Cross-Site Cookies&quot;, the authors note a pattern they call “Top-Level Cross-Site POST Requests.” The document recommends “Given the existing widespread usage and lack of clear alternatives, we recommend following the current state of the web and not blocking cross-site cookies in this scenario.”</td>
<td>This applies to any SAML SP that has 1. integrates using the recommended POST binding of the SAML response 2. uses SP initiated and saves state using cookies before sending the user for SAML authentication 3. and expects those cookies to be presented on the response in order to correlate the response to a session state with initial request parameters.</td>
</tr>
<tr>
<td><strong>IP address obfuscation</strong></td>
<td>Apple’s Private Relay for iCloud+ customers is a “lite” relay network used only with Safari and TCP Port 80 (aka http) traffic. All DNS requests are encrypted and go through Apple. Google has in October 2023 declared intent to obfuscate IP addresses of Chrome users. GoogleOne subscribers have access to Google VPN Mozilla offers a VPN</td>
<td>Apple’s relay is the most “friendly” providing details about the IP address ranges and documentation: Campus networks that need users on the network to not go through a relays but to appear to originate from the network must make changes documented at &quot;Prepare your network or web server for iCloud Private Relay.” Systems that assume region or city level geo-accuracy when interpreting IP address may only get country level accuracy if the user chooses that setting in the relay configuration. Google and Mozilla’s VPs do not seem to have published their final IP address ranges, nor any DNS to block in order to signal that VPN or relay use is unwelcome on the network. Google obfuscating the IP makes it unclear where the user is coming from.</td>
</tr>
<tr>
<td><strong>Robotic identification</strong></td>
<td>CAPTCHA solving is hard on mobile, challenging for accessibility reasons. Some CDNs essentially fingerprint browsers to distinguish “real” from &quot;bot&quot; surfing. <strong>Privacy Pass</strong> was introduced by Cloudflare (06/08/2022) and Apple (as Private Access Tokens). Work has been transferred to the IETF PrivacyPass working group. There are PrivacyPass plugins for Firefox and Chrome; believe its built into Safari. Web Environment Integrity API was announced by Google (2023-05-08) with a spec and explainer publicized (2023-07-21) and discussion (apparently) in the W3C Anti-Fraud Community Group.</td>
<td>No impact to federated authentication. Potential impact at sites that use CDNs to manage traffic.</td>
</tr>
</tbody>
</table>
Sites are identified by their server certificate, and then encrypt the transaction with an algorithm negotiated between server and client.

Authenticating the sites depends on the trust chain in the certificates. Google (as part of the “Moving Forward, Together” program) has proposed to the Certification Authority/Browser (CA/B) Forum that server certificates should have a 90 day certificate validity period.

Discussed at ACAMP in September 2023. Depending on how institutions and CAs manage certs, it may introduce confusion at least.

Chrome’s “Privacy Sandbox”, phasing out some third party cookies and including Shared Storage, starts general availability in Q3 2023


- "CHIPS: Allow developers to opt-in a cookie to partitioned storage, with a separate cookie jar per top-level site. CHIPS became available in Chrome Stable in February 2023."
- "Federated Credential Management (FedCM): Support federated identity without sharing the user’s email address or other identifying information with a third-party service or website, unless the user explicitly agrees to do so. FedCM shipped in November 2022."

Web Environment Integrity

Privacy Pass
- Thibault Meunier, Cloudflare https://www.usenix.org/conference/pepr23/presentation/meunier Tuesday, September 12, 2023 - 11:50 am–12:10 pm

We also have a collection of Slides, blogs, and videos from the community.

Useful references


