Privacy Sandbox

FedCM

Federated Credential Management

Facilitate seamless sign-in while safeguarding privacy

What's the privacy challenge?

Federated credentials allow people to sign in to various sites using their existing logins from Identity Providers, like social logins. This process enhances security and convenience for people while streamlining login management for businesses.

Currently, when someone visits a website with multiple login options, all of those providers may be notified about the visit, even if the user doesn't use their service to sign in. And some companies use this information to build out user profiles for advertising purposes.

Do things differently with FedCM

Make "Sign in with..." login solutions more private by shielding people's information and reducing passive tracking

User experience: FedCM helps streamline login solutions, leading to a smoother browsing experience for users.

Privacy-preserving data exchange: The login experience is handled by the browser, meaning that no information is shared with the site until a user wants it to be. Identity Providers also remain unaware of the user's online activity unless the user logs in with the service.

How it works

Step 1: Someone wants to log in to a site

Someone visits a site which requires them to log in or verify their identity for certain actions, like making a purchase or accessing premium content.

Step 2: FedCM is initiated

The site (known as the Relying Party) uses FedCM to allow people to easily sign in with an existing account from a trusted Identity Provider. The Relying Party chooses which Identity Providers to support on their site.

Step 3: Identity Provider is selected

The user selects their preferred Identity Provider from a dialog box in the browser. The site can't see the Identity Provider, and the Identity Providers can't see the site. The user's information stays with the browser until they log in with a service.

Step 4: Information is exchanged

Once the user initiates a login, the browser securely transmits the user's account selection to the Identity Provider, which verifies user credentials and generates a token. The token is validated, and the browser relays it to the Relying Party. Now that the user has accepted the FedCM prompt, the Relying Party and Identity Provider can share select information with each other via FedCM. The login credentials are not shared, but pertinent information like email address or profile picture can be shared for a more seamless site experience.

Step 5: The user is logged in and can continue their task on site

The user is now logged in to the site. Only the Identity Provider selected for login can communicate with the Relying Party, reducing the amount of information shared without the user's knowledge.

Learn more at goo.gle/fedcm