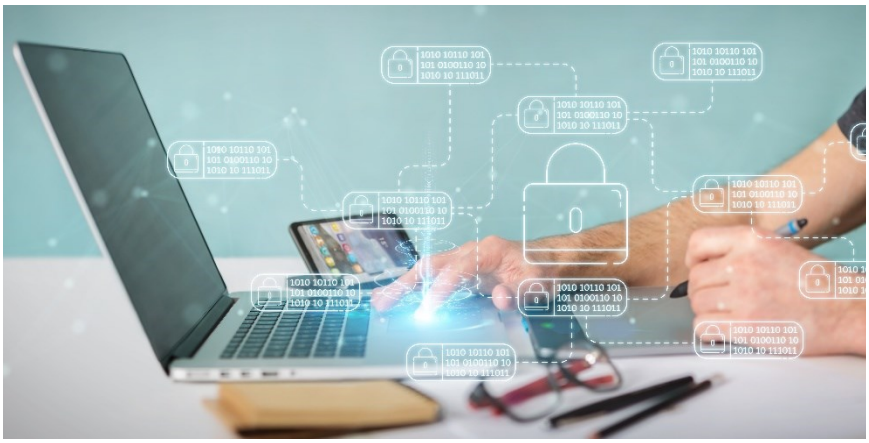
A-SIT

Secure Information Technology Center – Austria

Federated Credential Management

(FedCM API)



Federated Credential Management

Author:
Stefan More
Mail: stefan.more@a-sit.at
Date: December 2024

Browsers are introducing measures to improve user privacy. For example, in the future, users will be prevented from being tracked via "bounce redirects" and third-party cookies. However, these methods are also used in legitimate use cases, such as Federated Authentication/SSO, for example in OpenID Connect (OIDC). Therefore, there are several strategies to continue enabling these essential use cases.

One method is the Federated Credential Management (FedCM) API, which extends the JavaScript API of web browsers to enable Federated Authentication directly and with explicit user consent.

In this report, we evaluate FedCM and the impact on existing SSO systems. Specifically, the goal is to evaluate whether and to what extent FedCM can be used for SSO systems in the eGovernment environment (e.g., eIDAS, ID Austria), as they also rely on OIDC.

Inhalt

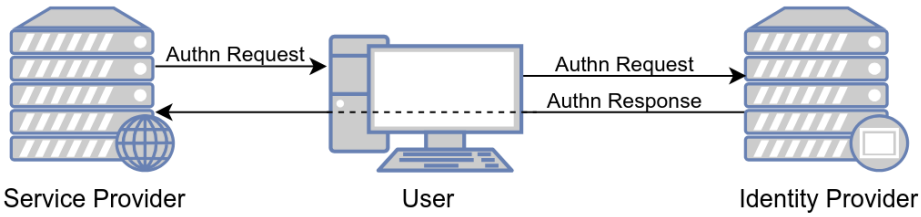
1. Introduction - 2 -
1.1. OpenID Connect - 2 -
1.2. Challenges - 2 -
1.3. ID Austria Analysis - 3 -
1.4. eIDAS Analysis - 4 -
2. Federated Credential Management API - 4 -
2.1. Technical Details - 4 -
2.2. Transition and Comparison - 5 -
3. Discussion - 5 -
3.1. Privacy Issues - 5 -
3.2. Standards Development - 5 -
3.3. Related Standards - 5 -
3.4. Compliance - 5 -
3.5. Improving FedCM's Privacy - 6 -
4. Conclusions - 6 -

1. Introduction

Federated authentication has emerged as a cornerstone of modern web interactions, enabling users to authenticate across multiple service providers (SPs) using a single identity provider (IDP). By reducing the need for multiple credentials, it streamlines user experiences and enhances security through centralized management of authentication protocols. This approach not only simplifies the login process but also minimizes password-related vulnerabilities, thereby contributing to a more secure and user-friendly digital ecosystem.

Examples include social login mechanisms provided by platforms like Google, Facebook, and Apple [5], OpenID Connect (OIDC) implementations [6], and government-provided E-ID initiatives such as ID Austria and the EU's eIDAS federation.

These systems simplify user experiences by reducing the need for multiple credentials, fostering secure and seamless access. Additionally, government-provided E-ID systems add value by providing government-attested identity attributes.



Basic authentication flow in federated authentication.

1.1. OpenID Connect

OpenID Connect (OIDC) is a widely adopted standard for federated authentication. It extends OAuth 2.0 by providing identity layers that allow applications to verify user identities and retrieve profile information. Government initiatives like ID Austria build on OIDC and integrate strong authentication mechanisms, ensuring secure access to eGovernment services. Similarly, the eIDAS federation seeks to standardize cross-border authentication within the European Union, promoting interoperability and trust based on national E-ID schemes.

1.2. Challenges

Federated authentication faces challenges, particularly as browser technologies evolve to enhance user privacy. Traditional mechanisms, such as bounce redirects and third-party cookies, are increasingly restricted due to their association with tracking:

- Bounce tracking, where users are redirected through third-party domains, faces mitigation strategies in modern browsers like Firefox and Chrome.
- Third-party cookies, integral to some OIDC flows, are being phased out under initiatives like Chrome's Privacy Sandbox and Firefox's Enhanced Tracking Protection.

These developments raise concerns as browsers are not inherently aware of legitimate use cases for these technologies, potentially disrupting federated authentication workflows.

Privacy concerns also arise from IDPs gaining visibility into user requests before user consent, creating potential for tracking [5].

To mitigate this issue and make sure that authentication solutions remain functional even after tracking technologies have been restricted, use case-aware browser interfaces have been proposed. One of these interfaces is the *Federated Credential Management API (FedCM)*.

It is thus needed to assess existing use cases building on specific technology that is also used for tracking. This situation further sparks a broader discussion about balancing protocol awareness in browsers with maintaining innovation and openness in the ecosystem.

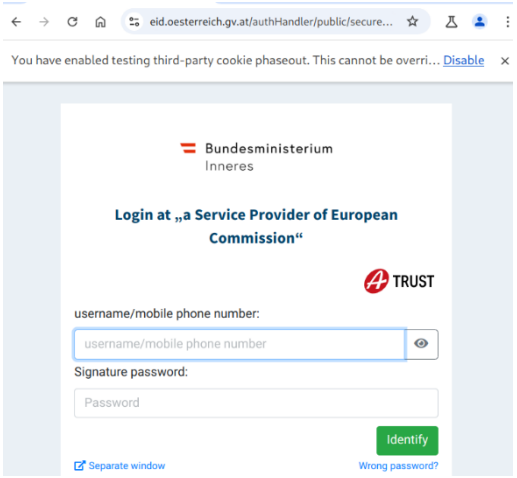
1.3. ID Austria Analysis

ID Austria, Austria's government-provided federated E-ID system, is at the moment resilient to modern privacy measures targeting bounce redirects and third-party cookies.

This resilience stems from its design, which mandates user login for every session and avoids relying on persistent login states at the IDP.

Testing with third-party cookie phase-out settings (e.g., Chrome's *-test-third-party-cookie-phaseout*) confirms its currently unaffected functionality. The system incorporates FIDO2 tokens as alternative for app-based authentication, which is currently also not affected by the mitigations.

1.4. eIDAS Analysis

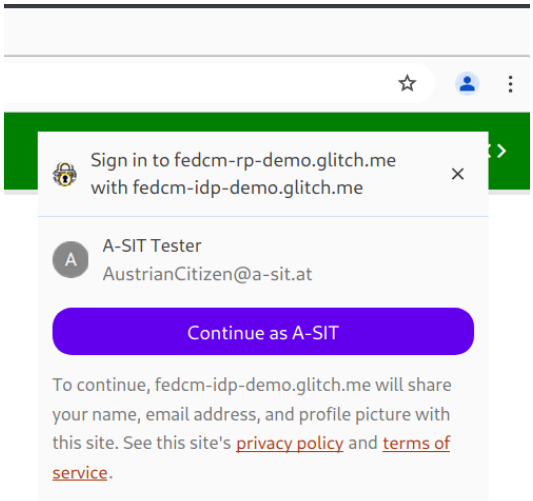


Like ID Austria, the eIDAS federated login, e.g., via EU Login, currently remains unaffected by bounce redirect and third-party cookie restrictions due to its reliance on fresh logins for each session. However, the federation's architecture includes multi-level redirects, which may require additional consideration in evolving browser environments. Preliminary tests indicate compatibility with third-party cookie phase-out measures, affirming its sustainability in the changing privacy landscape.

2. Federated Credential Management API

The Federated Credential Management API (FedCM) [7] represents a step towards modernizing federated authentication. Defined by W3C's Federated Identity Working Group, FedCM introduces a browser-integrated approach to managing user credentials. It aims to replace traditional mechanisms like third-party cookies and redirects used by systems like OIDC with a more privacy-conscious, user-centric model.

2.1. Technical Details



FedCM offers a JavaScript API, accessible through methods like *navigator.credentials.get()*, and a browser-mediated user interface.

It operates in two primary modes: Widget Mode (passive) and Button Mode (active). Widget Mode enables seamless authentication experiences, while Button Mode requires explicit user interaction. The active/button mode supports (re-)authentication of users, which is a requirement for ID Austria, as it authenticates the user on every login.

The API's design further ensures compatibility with mobile environments, catering to the increasing dominance of mobile platforms in web access.

2.2. Transition and Comparison

Compared to OpenID Connect, FedCM emphasizes privacy and browser-mediated control. For example, FedCM always requires user consent before initiating a connection to the IDP. This contrasts with OIDC, where interaction with the IDP's Login button already results in a connection to the IDP, thus leaking information about user behavior.

Transitioning to FedCM requires careful consideration. This consideration is aided by decision trees for implementers. It is further influenced by browser support timelines, and continuously progressing adjustments by IDPs and service providers (SPs). While FedCM holds promise, its adoption hinges on browser support and alignment with existing authentication ecosystems.

3. Discussion

3.1. Privacy Issues

Despite its advancements, FedCM is not immune to privacy concerns. Issues like linkability and observability persist [5], potentially undermining user trust.

3.2. Standards Development

Further, we highlight the potential for dominant players, such as Google, to even further influence the ecosystem, raising questions about centralized control and market dynamics in the web platform.

3.3. Related Standards

FedCM intersects with related standards like the Digital Credentials API and the Android Privacy Sandbox, which aim to enhance digital privacy.

3.4. Compliance

Compliance with the EU's ePrivacy Directive adds another layer of complexity, requiring user consent for activities involving access to user devices. This regulatory landscape necessitates meticulous adherence to privacy laws, as emphasized by FedCM's documentation.

3.5. Improving FedCM's Privacy

Enhancing FedCM's privacy features is a critical focus area. We thus recommend implementing privacy-preserving identifiers [3], such as pairwise pseudonymous identifiers outlined in the OpenID Connect specifications. This is supported by reports by Mozilla that emphasize the importance of IdP blindness and directed identifiers, which limit unnecessary exposure of user information

Research efforts like our BISON [1] or the OPPID technology [2] provide strategies for achieving robust privacy.

4. Conclusions

The Federated Credential Management API presents a compelling opportunity for modernizing federated authentication. However, its adoption depends on changes by service providers and IDPs, as well as widespread browser support. Currently, Chrome leads in implementation, with Mozilla prototyping and other browsers lagging.

The urgency of FedCM's adoption is tempered by the postponement of third-party cookie deprecation and the potential of alternative solutions like wallets and digital credential APIs to address prevailing challenges. As the ecosystem evolves, FedCM must align with user privacy expectations and regulatory requirements to achieve its full potential.

References

[*] OpenAI. ChatGPT (4o) [Large language model] was used to edit parts of the text.

[1] Jakob Heher, Stefan More, Lena Heimberger, BISON: Blind Identification with Stateless scOped pseudoNyms. arXiv pre-print, 2024.

[2] Maximilian Kroschewski, Anja Lehmann, Cavit Özbay, OPPID: Single Sign-On with Oblivious Pairwise Pseudonyms. Cryptology ePrint Archive, 2024.

[3] Stefan More, Privacy-Preserving Identifiers. Report, 2024. https://technology.a-sit.at/en/privacy-preserving-identifiers/

[4] Apple, Authenticating users with "Sign in with Apple". https://developer.apple.com/documentation/sign_in_with_apple/sign_in_with_apple_rest_api/authenticating_users_with_sign_in_with_apple, retrieved Sept 2023.

[5] A. Pfitzmann, M. Hansen. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology (Version 0.28), 2006.

[6] Nat Sakimura, John Bradley, Michael B. Jones, Breno de Medeiros, Chuck Mortimore, OpenID Connect Core 1.0. https://openid.net/specs/openid-connect-core-1_0.html, 2014.

[7] Nicolás Peña Moreno, Sam Goto, Federated Credential Management API (Working Draft). https://www.w3.org/TR/fedcm, August 2024.