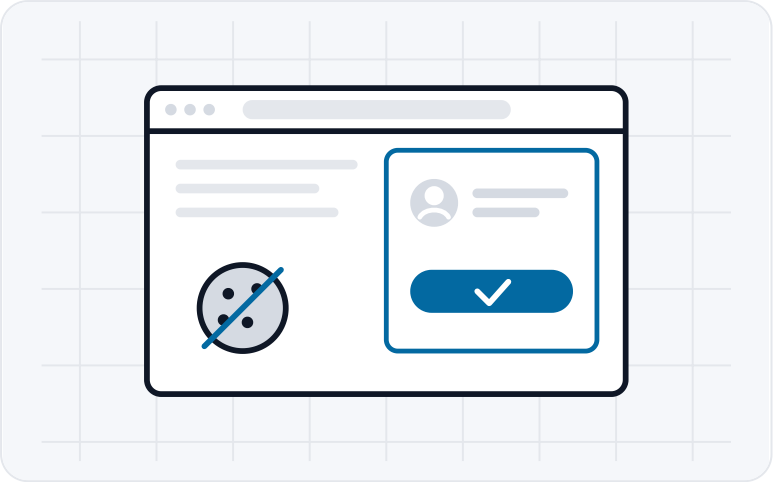
A-SIT Technology

E-Government Innovationszentrum

23. Dezember 2024 Analyse · Digitale Identität · Web & Cloud

Federated Credential Management (FedCM API)

Stefan More



Autorinnen und Autoren	Stefan More
Quelle	https://technology2.a-sit.at/veroeffentlichungen/federated-credential-management-fedcm-api/
Hinweis	Maschinell übersetzt.

Kernaussagen

- ID Austria ist laut Tests mit abgeschalteten Third-Party-Cookies derzeit unbeeinträchtigt, weil bei jeder Sitzung eine neue Anmeldung nötig ist.
- Die eIDAS-Föderation ist derzeit ebenfalls unberührt; mehrstufige Weiterleitungen sind in sich entwickelnden Browsern zusätzlich zu beachten.
- FedCM verlangt stets die Einwilligung der Benutzer, bevor eine Verbindung zum IDP aufgebaut wird; bei OIDC genügt schon die Interaktion mit dem Login-Button.
- FedCM hat weiterhin Datenschutzprobleme (Linkability, Observability); empfohlen werden Pairwise Pseudonymous Identifiers.
- Die Einführung von FedCM hängt von Änderungen bei SPs und IDPs und von breiter Browserunterstützung ab; Chrome führt, Mozilla entwickelt einen Prototyp.

Browser führen Maßnahmen ein, um die Privatsphäre von Benutzern zu verbessern. Beispielsweise wird in Zukunft verhindert, das User mittels „Bounce Redirects“ und 3rd Party Cookie getracked werden. Diese Methoden werden aber auch von legitimen Use Cases verwendet, zB Federated Authentication/SSO beispielsweise in OpenID Connect (OIDC). Daher gibt es mehrere Strategien, um diese essentiellen Use Cases weiterhin zu ermöglichen.

Eine Methode ist die Federated Credential Management (FedCM) API, welche die Javascript API von Webbrowsern erweitert, um Federated Authentication direkt und mit explizitem user consent zu ermöglichen.

Im Rahmen dieses Berichts wird FedCM analysiert. Im Speziellen wird evaluiert, ob bzw. in welchem Ausmaß sich FedCM für SSO Systeme im eGovernment Umfeld (zB eIDAS, ID Austria) verwenden lässt, da diese auch auf OIDC setzen.

1. Einleitung

Federated Authentication hat sich zu einem Eckpfeiler moderner Web-Interaktionen entwickelt. Sie ermöglicht es Benutzern, sich bei mehreren Service Providern (SPs) mit einem einzigen Identity Provider (IDP) zu authentifizieren. Da weniger Zugangsdaten nötig sind, vereinfacht sie die Benutzererfahrung und erhöht durch die zentrale Verwaltung der Authentifizierungsprotokolle die Sicherheit. Dieser Ansatz vereinfacht nicht nur den Anmeldevorgang, sondern verringert auch passwortbezogene Schwachstellen und trägt so zu einem sichereren und benutzerfreundlicheren digitalen Ökosystem bei.

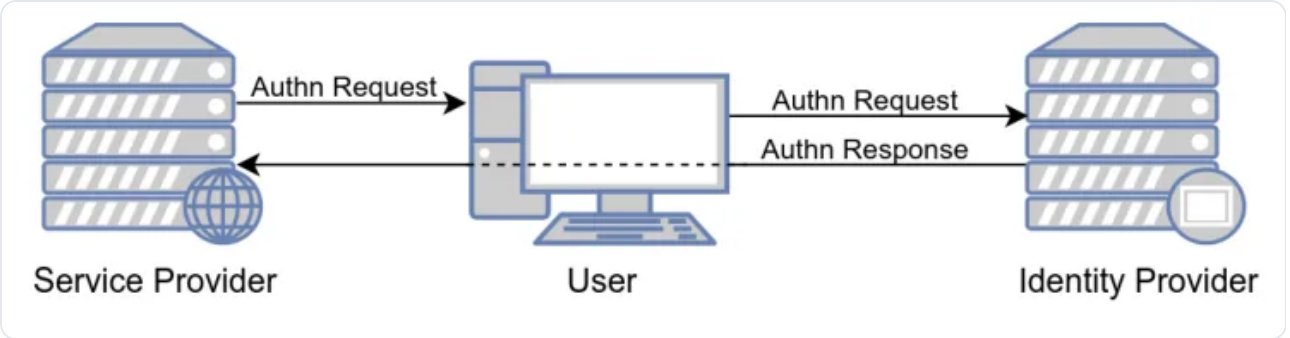
Beispiele sind Social-Login-Mechanismen von Plattformen wie Google, Facebook und Apple [5], OpenID-Connect-(OIDC-)Implementierungen [6] sowie staatlich bereitgestellte E-ID-Initiativen wie ID Austria und die eIDAS-Föderation der EU.

Diese Systeme vereinfachen die Benutzererfahrung, indem sie den Bedarf an mehreren Zugangsdaten verringern, und fördern einen sicheren und nahtlosen Zugang. Zusätzlich bieten staatlich bereitgestellte E-ID-Systeme einen Mehrwert, da sie staatlich bestätigte Identitätsattribute liefern.

1.1. OpenID Connect

OpenID Connect (OIDC) ist ein weit verbreiteter Standard für Federated Authentication. Er erweitert OAuth 2.0 um Identitätsschichten, mit denen Anwendungen die Identität von Benutzern überprüfen und Profilinformationen abrufen können. Staatliche Initiativen wie ID Austria bauen auf OIDC auf und integrieren starke Authentifizierungsmechanismen, die einen sicheren Zugang zu eGovernment-Diensten gewährleisten. Ebenso strebt die eIDAS-Föderation an, die grenzüberschreitende Authentifizierung innerhalb der Europäischen Union zu standardisieren und auf Basis nationaler E-ID-Systeme Interoperabilität und Vertrauen zu fördern.

1.2. Herausforderungen



Grundlegender Authentifizierungsablauf bei Federated Authentication.

Federated Authentication steht vor Herausforderungen, insbesondere weil sich Browsertechnologien weiterentwickeln, um die Privatsphäre der Benutzer zu stärken. Herkömmliche Mechanismen wie Bounce Redirects und Third-Party-Cookies werden zunehmend eingeschränkt, da sie mit Tracking in Verbindung stehen:

- Gegen Bounce Tracking, bei dem Benutzer über Domains Dritter umgeleitet werden, gibt es in modernen Browsern wie Firefox und Chrome bereits Gegenmaßnahmen.
- Third-Party-Cookies, die für manche OIDC-Abläufe unverzichtbar sind, werden im Rahmen von Initiativen wie Chromes Privacy Sandbox und Firefox' Enhanced Tracking Protection schrittweise abgeschafft.

Diese Entwicklungen geben Anlass zur Sorge, da Browser legitime Anwendungsfälle dieser Technologien nicht von sich aus erkennen. Dadurch können Federated-Authentication-Abläufe gestört werden.

Datenschutzbedenken ergeben sich auch daraus, dass IDPs Anfragen von Benutzern bereits vor der Einwilligung einsehen können, was Tracking ermöglichen kann [5].

Um dieses Problem zu entschärfen und sicherzustellen, dass Authentifizierungslösungen auch nach der Einschränkung von Tracking-Technologien funktionsfähig bleiben, wurden anwendungsfallbezogene Browser-Schnittstellen vorgeschlagen. Eine dieser Schnittstellen ist die Federated Credential Management API (FedCM).

Daher müssen bestehende Anwendungsfälle untersucht werden, die auf bestimmten Technologien aufbauen, welche auch für Tracking verwendet werden. Diese Situation löst zudem eine breitere Diskussion darüber aus, wie sich die Protokollkenntnis von Browsern mit der Wahrung von Innovation und Offenheit im Ökosystem vereinbaren lässt.

1.3. ID-Austria-Analyse

ID Austria, das staatlich bereitgestellte Federated-E-ID-System Österreichs, ist derzeit gegenüber modernen Datenschutzmaßnahmen gegen Bounce Redirects und Third-Party-Cookies widerstandsfähig.

Diese Widerstandsfähigkeit ergibt sich aus dem Design: Es schreibt für jede Sitzung eine Anmeldung der Benutzer vor und verzichtet auf dauerhafte Anmeldezustände beim IDP.

Tests mit Einstellungen zur Abschaffung von Third-Party-Cookies (z. B. Chromes -test-third-party-cookiephaseout) bestätigen, dass die Funktion derzeit unbeeinträchtigt ist. Das System integriert FIDO2-Tokens als Alternative zur App-basierten Authentifizierung, die von den Maßnahmen derzeit ebenfalls nicht betroffen ist.

1.4. eIDAS-Analyse

Wie ID Austria bleibt auch die eIDAS-Federated-Anmeldung, z. B. über EU Login, von den Einschränkungen für Bounce Redirects und Third-Party-Cookies derzeit unberührt, da für jede Sitzung eine neue Anmeldung erforderlich ist. Die Architektur der Föderation umfasst jedoch mehrstufige Weiterleitungen, die in sich entwickelnden Browserumgebungen zusätzlich berücksichtigt werden müssen. Vorläufige Tests deuten auf Kompatibilität mit den Maßnahmen zur Abschaffung von Third-Party-Cookies hin und bestätigen damit die Tragfähigkeit in der sich wandelnden Datenschutzlandschaft.

2. Federated Credential Management API

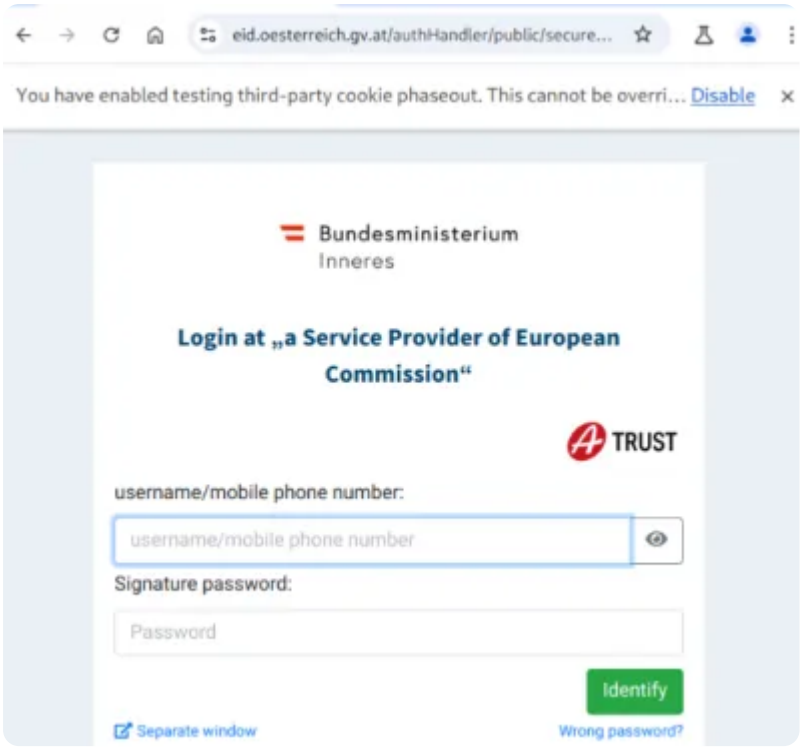
Die Federated Credential Management API (FedCM) [7] stellt einen Schritt zur Modernisierung der Federated Authentication dar. FedCM wird von der Federated Identity Working Group des W3C definiert und führt einen in den Browser integrierten Ansatz zur Verwaltung von Benutzer-Credentials ein. Sie soll herkömmliche Mechanismen wie Third-Party-Cookies und Redirects, die Systeme wie OIDC verwenden, durch ein datenschutzfreundlicheres, benutzerzentriertes Modell ersetzen.

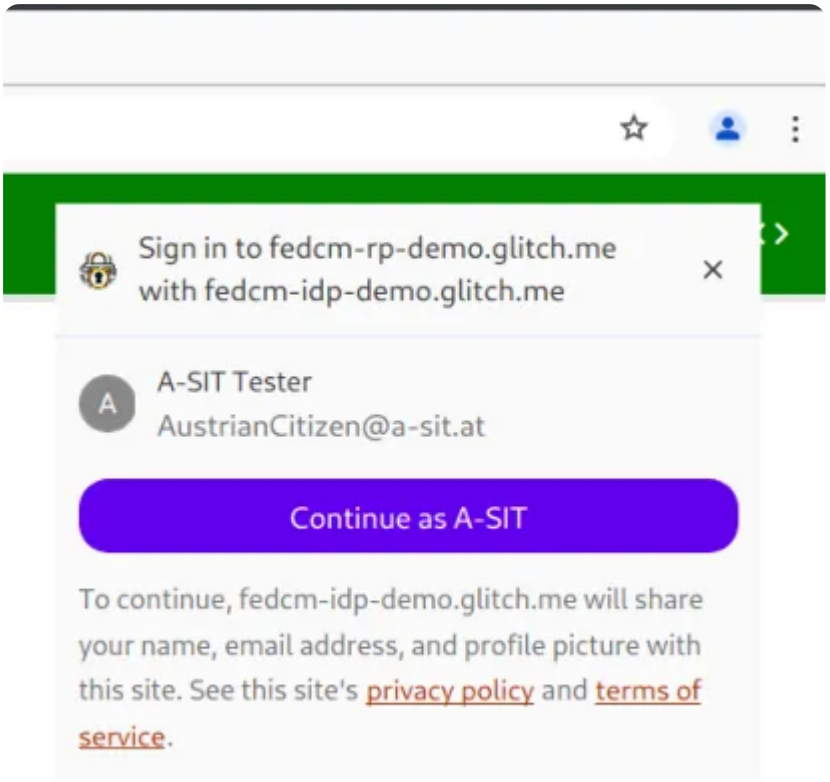
2.1. Technische Details

FedCM bietet eine JavaScript-API, die über Methoden wie navigator.credentials.get() zugänglich ist, sowie eine vom Browser vermittelte Benutzeroberfläche.

Sie arbeitet in zwei Hauptmodi: Widget Mode (passiv) und Button Mode (aktiv). Der Widget Mode ermöglicht nahtlose Authentifizierungsabläufe, während der Button Mode eine ausdrückliche Benutzerinteraktion erfordert. Der aktive Modus (Button Mode) unterstützt die (erneute) Authentifizierung von Benutzern. Das ist eine Anforderung von ID Austria, da dort bei jeder Anmeldung eine Authentifizierung erfolgt.

Das Design der API gewährleistet zudem Kompatibilität mit mobilen Umgebungen und trägt damit der zunehmenden Dominanz mobiler Plattformen beim Webzugriff Rechnung.





2.2. Übergang und Vergleich

Im Vergleich zu OpenID Connect legt FedCM den Schwerpunkt auf Privatsphäre und browservermittelte Kontrolle. So verlangt FedCM stets die Einwilligung der Benutzer, bevor eine Verbindung zum IDP aufgebaut wird. Dies steht im Gegensatz zu OIDC, wo bereits die Interaktion mit dem Login-Button des IDP eine

Verbindung zum IDP herstellt und dadurch Informationen über das Benutzerverhalten preisgibt.

Der Übergang zu FedCM erfordert sorgfältige Überlegung. Dabei helfen Entscheidungsbäume für Implementierende. Sie wird zudem von den Zeitplänen der Browserunterstützung und von laufenden Anpassungen durch IDPs und Service Provider (SPs) beeinflusst. FedCM ist vielversprechend, doch ihre Einführung hängt von der Browserunterstützung und der Abstimmung mit bestehenden Authentifizierungs-Ökosystemen ab.

3. Diskussion

3.1. Datenschutzprobleme

Trotz ihrer Fortschritte ist FedCM nicht frei von Datenschutzproblemen. Probleme wie Linkability und Observability bestehen weiterhin [5] und können das Vertrauen der Benutzer untergraben.

3.2. Standardentwicklung

Wir weisen außerdem darauf hin, dass dominante Akteure wie Google das Ökosystem noch stärker beeinflussen könnten. Das wirft Fragen zu zentraler Kontrolle und Marktdynamik auf der Webplattform auf.

3.3. Verwandte Standards

FedCM überschneidet sich mit verwandten Standards wie der Digital Credentials API und der Android Privacy Sandbox, die den digitalen Datenschutz verbessern sollen.

3.4. Compliance

Die Einhaltung der ePrivacy-Richtlinie der EU erhöht die Komplexität zusätzlich, da für Tätigkeiten mit Zugriff auf Endgeräte der Benutzer eine Einwilligung erforderlich ist. Diese regulatorische Lage erfordert die sorgfältige Einhaltung der Datenschutzgesetze, wie auch die Dokumentation von FedCM betont.

3.5. Verbesserung der Privatsphäre in FedCM

Die Stärkung der Datenschutzfunktionen von FedCM ist ein zentrales Handlungsfeld. Daher wird empfohlen, privatsphärenschützende Identifikatoren [3] einzusetzen, etwa paarweise pseudonyme Identifikatoren (Pairwise Pseudonymous Identifiers), wie sie in den OpenID-Connect-Spezifikationen beschrieben sind. Dies wird durch Berichte von Mozilla gestützt, die die Bedeutung von IdP Blindness und Directed Identifiers hervorheben, welche die unnötige Offenlegung von Benutzerinformationen begrenzen. Forschungsarbeiten wie unser BISON [1] oder die OPPID-Technologie [2] bieten Strategien für einen robusten Datenschutz.

4. Schlussfolgerungen

Die Federated Credential Management API bietet eine überzeugende Gelegenheit, Federated Authentication zu modernisieren. Ihre Einführung hängt jedoch von Änderungen bei Service Providern und IDPs sowie von einer breiten Browserunterstützung ab. Derzeit führt Chrome bei der Umsetzung, Mozilla entwickelt einen Prototyp, und andere Browser liegen zurück. Die Dringlichkeit der Einführung von FedCM wird dadurch gemildert, dass die Abschaffung von Third-Party-Cookies verschoben wurde und

Alternativen wie Wallets und Digital-Credential-APIs die bestehenden Herausforderungen lösen könnten. Mit der Weiterentwicklung des Ökosystems muss FedCM sich an den Erwartungen der Benutzer an die Privatsphäre und an regulatorischen Anforderungen ausrichten, um ihr volles Potenzial zu entfalten.

Literaturverzeichnis

[*] 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.