A-SIT Technology

E-Government Innovationszentrum

31. Oktober 2025 Überblick · Web & Cloud · Digitale Identität · 22 Min. Lesezeit

Web APIs für Identitätsmanagement

Stefan More



Autorinnen und Autoren	Stefan More
Quelle	https://technology2.a-sit.at/veroeffentlichungen/web-apis-fuer-identitaetsmanagement/
Hinweis	Maschinell übersetzt.

Kernaussagen

- FedCM und WebAuthn/FIDO2 sind ausgereift genug für den heutigen Einsatz und können Sicherheit und Datenschutz nationaler eID-Systeme verbessern.
- Die Digital Credentials API wird mit VC 2.0 und OID4VCI bzw. OID4VP zum zentralen Webstandard-Stack für Wallet-basierte Identität unter eIDAS 2.
- FedCM bleibt IdP-zentriert, der IdP sieht jedes Authentifizierungsereignis; BISON-Pseudonyme könnten Tracking verringern, sind aber (noch) kein Standard.
- Die Digital Credentials API wird in Chrome, Safari und Android implementiert; in Chrome ist sie ab Version 141 allgemein verfügbar.
- Öffentliche Verwaltungen sollten DC-API-basierte Lösungen als strategisch wichtig, kurzfristig aber nicht als alleinige Grundlage betrachten.

Web-Browser und die Web-Standardisierungs Community führen laufend neue Webbrowser Schnittstellen für diverse Anwendungsfälle ein. Im speziellen interessant sind hier APIs (Application Programming Interface) für Identitätsmanagement (IDM).

Bisher findet Identitätsmanagement im Browser primär auf Basis generischer Web-Technologien (HTML, Cookies, Redirects, ...) statt, und wird nun durch die neuen Schnittstellen tiefer in den Browser integriert. Dies stellt die gewünschte Funktionalität auch bei steigenden Privatsphäre Anforderungen und restriktiveren Webbrowsern sicher (zB Einschränkung von „Bounce Redirects“ und „Third-Party Cookies“). Des weiteren ermöglichen IDM-spezifische Browser-APIs neue Anwendungsfälle, wie beispielsweise eine tiefere Integration in das Betriebssystem oder Zugriff auf Hardware.

Beispiele für diese IDM-spezifischen Web-APIs sind die Digital Credentials API (DC API), Federated Credential Management (FedCM), und die Web Authentication API (WebAuthn).

Im Rahmen dieses Projektes werden aktuelle APIs analysiert und der Entwicklungsstand evaluiert. Des weiteren werden aktuelle Entwürfe und Diskussionen im Bereich IDM-spezifischer Webstandards untersucht.

1. Einleitung

1.1. Motivation und Umfang

Identitätsmanagement (IDM) im Web entwickelt sich von Ad-hoc-Seitenabläufen hin zu expliziten Web-Plattform-APIs. Historisch nutzten Single-Sign-on-Lösungen (SSO) und eGovernment-Login-Lösungen protokollspezifische Redirects, Cookies und versteckte iframes, um SAML- und OpenID-Connect-Abläufe (OIDC) umzusetzen. Diese Mechanismen geraten nun durch Datenschutzmaßnahmen wie Tracking-Schutz und die Abschaffung von Third-Party-Cookies unter Druck. Außerdem erfordern neue Paradigmen des Identitätsmanagements (z. B. SSSI, Wallets) eine tiefere Integration in den Browser.

Als Reaktion darauf definieren Browser-Hersteller und Standardisierungsgremien identitätsspezifische Web-APIs, z. B.

- Federated Credential Management API (FedCM): browservermittelte Authentifizierungsföderation
- Web Authentication API (WebAuthn) und FIDO2 bzw. Passkeys für phishing-resistente Authentifizierung
- Digital Credentials API (DC API): Präsentation und Ausstellung digitaler Nachweise aus Wallets

Dieser Bericht konzentriert sich auf diese APIs als Webstandards und nicht auf bestimmte Produkte einzelner Hersteller oder nationale Implementierungen. Er analysiert ihre Eignung als Bausteine für Identitätssysteme der öffentlichen Verwaltung.

1.2. Regulatorischer und eGovernment-Kontext

Im April 2024 verabschiedete die Europäische Union die Verordnung (EU) 2024/1183 (eIDAS 2), die die Verordnung (EU) Nr. 910/2014 (eIDAS) ändert und einen europäischen Rahmen für eine digitale Identität schafft [5]. Dieser Rahmen führt die European Digital Identity Wallet (EUDI Wallet) als harmonisiertes Mittel zur elektronischen Identifizierung und zum Austausch von Attributen zwischen den Mitgliedstaaten ein. Ab Ende 2026 muss jeder Mitgliedstaat mindestens eine Wallet für natürliche und juristische Personen bereitstellen.

Die technische Umsetzung dieses Rahmens wird in der European Digital Identity Architecture and Reference Framework (EUDI ARF) beschrieben. Das ARF verweist auf mehrere Webstandards, insbesondere:

- Verifiable Credentials Data Model [7]
- OpenID for Verifiable Credential Issuance (OID4VCI) [8] und OpenID for Verifiable Presentations (OID4VP) [9]
- die Digital Credentials API als möglicher Wallet-Browser-Schnittstelle für Remote-Abläufe im Browser [6,15]

Das österreichische nationale eID-System (eIDAS 1), ID Austria, ist bereits im Produktivbetrieb und verwendet OpenID Connect und SAML 2.0 zur Anbindung von Diensteanbietern [16]. Es bietet außerdem eine qualifizierte elektronische Signatur (QES), die in der gesamten EU rechtlich einer handschriftlichen Unterschrift gleichgestellt ist [17]. ID Austria baut auf einem smartphonegestützten Authentifizierungsfaktor auf, unterstützt aber auch FIDO2-Token mit WebAuthn als zweiten Faktor [18].

Dieser Bericht verwendet ID Austria als konkretes Beispiel für eine bestehende eID-Lösung und EUDI-Wallets als zukunftsorientierte Architektur unter eIDAS 2.

2. Hintergrund: Identitätsmanagement im Web

Das Internet wurde ohne Identitätsschicht gebaut.

— Kim Cameron, (Microsoft Chief Identity Architect, The Laws of Identity, Mai 2005)

2.1. Klassisches Web-Single-Sign-on

Klassisches Web-Single-Sign-on (SSO) wird typischerweise durch die Kombination folgender Elemente umgesetzt:

- HTTP-Redirects zwischen der Relying Party (RP) und dem Identity Provider (IdP)
- vom Browser verwaltete Cookies auf beiden Seiten zur Aufrechterhaltung von Sitzungen
- HTML- oder skriptbasierte Abläufe (einschließlich versteckter iframes) zum Austausch von Protokollnachrichten

Die vorherrschenden Protokolle sind Security Assertion Markup Language (SAML) 2.0 und OpenID Connect Core 1.0 (OIDC). OIDC standardisiert die Authentifizierung auf Basis von OAuth 2.0, verwendet signierte JSON Web Tokens (ID Tokens) und unterstützt Discovery und dynamische Client-Registrierung [1]. SAML 2.0 ist im öffentlichen Sektor weit verbreitet und gilt als ausgereift und relativ statisch.

Dieses Modell ist flexibel und erfordert keine explizite Browser-Unterstützung, weist aber mehrere Einschränkungen auf:

- Privatsphäre und Tracking: Seitenübergreifende Cookies und eingebettete Ressourcen können nicht nur zur Authentifizierung, sondern auch zum Tracking von Nutzenden verwendet werden. Das ist besonders problematisch, wenn große IdPs von vielen RPs genutzt werden (z. B. Google oder die Bundesverwaltung).
- Komplexe Abläufe: Anwendungsentwickelnde müssen protokollspezifische Redirects und Fehlerbehandlung explizit umsetzen und die Kommunikation mit jedem IdP einzeln ermöglichen.
- Geräteübergreifende Abläufe: Redirect-basierte Abläufe sind umständlich, wenn Nutzende eine Transaktion auf einem Gerät beginnen und auf einem anderen abschließen. Das ist eine Herausforderung für Anwendungsfälle, die auf der Desktop-Nutzung aufbauen, aber das Smartphone als zweiten Faktor oder zur Verwaltung von Identitätsnachweisen (Wallet) benötigen.

2.2. Bausteine der Webstandards

Um diese Probleme zu adressieren, sind mehrere Web-Plattform-Standards entstanden.

Credential Management API

Die Credential Management API definiert generische Schnittstellen zur Speicherung und zum Abruf von Credentials in Browsern. Sie unterstützt Passwort-Credentials, föderierte Credentials und Public-Key-Credentials und bildet die Basis, auf der WebAuthn und die Digital Credentials API aufbauen.

Web Authentication API (WebAuthn) und FIDO2

WebAuthn definiert eine API zum Erstellen und Verwenden von Public-Key-basierten Credentials, die an Authenticatoren gebunden sind, mit Attestation und Origin-Bindung [10]. Zusammen mit dem Client to Authenticator Protocol (CTAP) der FIDO Alliance bildet sie den FIDO2-Standard und ist die Grundlage für Passkeys. Passkeys sind auffindbare (discoverable) WebAuthn-Credentials, die in Betriebssysteme integriert sind und zwischen Geräten synchronisiert werden.

Federated Credential Management API (FedCM)

FedCM ist eine Spezifikation der W3C Federated Identity Working Group, die eine browservermittelte API für föderierte Anmeldung definiert. Sie soll die Vorteile der Identitätsföderation erhalten und gleichzeitig die Abhängigkeit von Third-Party-Cookies und intransparenten Redirects beseitigen [1,22].

Digital Credentials API[1] (DC API)

Die Digital Credentials API erweitert die Credential Management API, damit User Agents die Präsentation und Ausstellung digitaler Nachweise (wie Ausweise oder Führerscheine) aus zugrunde liegenden Plattformen oder Wallets vermitteln können [3].

Diese APIs werden durch Daten- und Protokollstandards ergänzt: das Verifiable Credentials Data Model v2.0, eine W3C Recommendation zur formatunabhängigen Darstellung von Verifiable Credentials [7]. Dazu kommen OpenID for Verifiable Credential Issuance (OID4VCI) und OpenID for Verifiable Presentations (OID4VP), die OAuth-basierte APIs zur Ausstellung und Präsentation von Credentials spezifizieren und den Transport über die Digital Credentials API ausdrücklich unterstützen [8,9].

2.3. eIDAS 2 und die European Digital Identity Wallet

Die Verordnung (EU) 2024/1183 ändert die eIDAS-1-Verordnung, um einen europäischen Rahmen für eine digitale Identität zu schaffen, in dem die Mitgliedstaaten mindestens eine European Digital Identity Wallet anbieten müssen. Die Wallet ist ein Softwareprodukt, das von einem Mitgliedstaat ausgegeben (oder anerkannt) wird. Eine Wallet ermöglicht es Nutzenden, sich online und offline zu identifizieren, sich gegenüber Relying Parties (RPs) zu authentifizieren und Attribute und Credentials zu präsentieren, die von öffentlichen und privaten Stellen ausgestellt wurden [5].

Das EUDI Architecture and Reference Framework (ARF) spezifiziert technische Bausteine. Für Web-Interaktionen nennt es:

- VC 2.0 und verwandte W3C-Standards als Datenmodell für Credentials
- OID4VCI und OID4VP als bevorzugte Protokolle für Ausstellung und Präsentation
- die Digital Credentials API als mögliche Plattform-API zwischen der Wallet-Einheit und dem Browser bzw. Betriebssystem für Remote-Abläufe [6,15]

3. Webstandards für browservermittelte Identität

3.1. Federated Credential Management (FedCM)

3.1.1. Überblick und Standardisierungsstatus

Die Federated Credential Management API (FedCM) wird von der W3C Federated Identity Working Group als browservermittelte Alternative zur klassischen föderierten Anmeldung auf Basis von Redirects und Third-Party-Cookies definiert [1]. Stand Oktober 2025 ist die aktuelle Spezifikation ein First Public Working Draft auf dem W3C-Recommendation-Track. Die Working Group beabsichtigt, sie zur Recommendation weiterzuentwickeln, sobald ausreichend Implementierungserfahrung vorliegt.

Die MDN beschreibt FedCM als "einen Standardmechanismus für Identity Provider, um Identitätsföderationsdienste im Web datenschutzfreundlich bereitzustellen, ohne Third-Party-Cookies und Redirects" [22]. Chromium-basierte Browser implementieren FedCM bereits, und große Identity Provider, darunter Google, haben ihre Anmeldeabläufe darauf umgestellt.

3.1.2. Protokollmodell und Architektur

FedCM führt eine JavaScript-API (`navigator.credentials.get()` mit föderierten Optionen) und eine vom Browser kontrollierte Kontoauswahl-Oberfläche ein. In einem vereinfachten FedCM-Ablauf:

1. Die Relying Party (RP) ruft die FedCM-API mit Informationen über unterstützte Identity Provider (IdPs) und angeforderte Scopes auf.
2. Der Browser fragt die von FedCM und dem zugrunde liegenden Protokoll definierten Konfigurations-Endpunkte des IdP ab, gegebenenfalls unter Verwendung der Login Status API für Kontoinformationen.
3. Der Browser zeigt den Nutzenden einen nativen Dialog mit Konten und Berechtigungen an.
4. Nach Zustimmung der Nutzenden holt der Browser eine Assertion (zum Beispiel ein OIDC ID Token) vom IdP und gibt sie an die RP zurück.

FedCM ist bewusst protokollunabhängig. In der Praxis ist OIDC das primäre zugrunde liegende Protokoll, die Working Group legt jedoch Wert darauf, protokollspezifische Logik außerhalb der FedCM-Spezifikation zu halten.

Ein verwandter Vorschlag, oft als Lightweight FedCM bezeichnet, diskutiert die Vereinfachung der IdP-Integration, zum Beispiel indem IdPs Kontoinformationen über die Login Status API an den Browser übermitteln. Dies wird in der FedID Community Group und Working Group noch diskutiert.

3.1.3. Datenschutz- und Sicherheitseigenschaften

FedCM soll Datenschutz (und Sicherheit) gegenüber klassischem Redirect-basiertem SSO verbessern:

- Zustimmung und Datenschutz: Da der Anmeldeablauf vom Browser vermittelt wird, behalten die Nutzenden die Kontrolle über den Ablauf. Der IdP erfährt erst von den Absichten der Nutzenden, wenn diese der Anmeldung zugestimmt haben. Dieser Ablauf ermöglicht auch Tracking-Schutzmechanismen wie BISON (siehe unten).

- Vom Browser vermittelte Oberfläche: Die Kontoauswahl wird vom Browser kontrolliert, was die Möglichkeiten für irreführende gefälschte Anmeldeseiten verringert.

- Partitionierter Zustand: FedCM ist darauf ausgelegt, ohne Third-Party-Cookies zu funktionieren. Der IdP-Zustand wird pro RP oder pro Top-Level-Site partitioniert, entsprechend den Tracking-Schutzmechanismen.

- Begrenzter Metadatenabfluss: Die FedID Working Group und Community Group diskutieren Timing-Angriffe und Caching-Strategien, um zu vermeiden, dass offengelegt wird, bei welchen RPs sich Nutzende anmelden [1].

FedCM bleibt jedoch IdP-zentriert. Der IdP sieht weiterhin jedes Authentifizierungsereignis. Um IdP-basiertes dienstübergreifendes Tracking zu verhindern, sind sorgfältig gestaltete Identifikatoren und Richtlinien nötig.

3.1.4. Relevanz für eGovernment

Für eGovernment-Systeme wie ID Austria könnte FedCM als modernisiertes Front-End für das bestehende OIDC-basierte Login dienen:

- Die OIDC-Endpunkte und Discovery-Dokumente von ID Austria sind öffentlich [16].
- Grundsätzlich könnte ID Austria eine FedCM-Konfiguration für ihre OIDC-Endpunkte bereitstellen, sodass Browser eine native Erfahrung „Mit ID Austria anmelden" bieten können.

Das würde die Vorteile der Föderation ohne Third-Party-Cookies erhalten, die Benutzererfahrung durch eine einheitliche Browser-Oberfläche verbessern und die Abhängigkeit von fragilen Redirect- oder Cookie-Abläufen verringern. Für die grenzüberschreitende Nutzung im Rahmen des alten eIDAS-Node-Modells könnte FedCM ähnlich mit nationalen IdPs eingesetzt werden.

In einer wallet-zentrierten EUDI-Welt ist FedCM weniger relevant als die Digital Credentials API.

3.1.5. Datenschutzerweiterung: BISON-Pseudonyme

Das BISON-Protokoll von A-SIT („Blind Identification with Stateless scOped pseudoNyms") schlägt einen Weg vor, mit Kryptografie und Oblivious Pseudorandom Functions pro RP eigene Pseudonyme abzuleiten [19]. Es ist darauf ausgelegt, sich in bestehende Protokolle (insbesondere OIDC) zu integrieren, und verbirgt die Identität der RP vor dem IdP, während es dennoch stabile, auf die RP bezogene Identifikatoren erzeugt.

Außerdem bietet BISON:

- eine OIDC-Erweiterung, die BISON für paarweise pseudonyme Identifikatoren verwendet
- Prototyp-Implementierungen für IdP und RP sowie eine Firefox-Erweiterung, die die erforderliche Browser-Unterstützung simuliert [20]

Obwohl BISON (noch?) kein Standard ist, zeigt es, wie FedCM-plus-OIDC-Einsätze künftig eine browservermittelte Benutzererfahrung mit starken kryptografischen Datenschutzgarantien für hochsensible eGovernment-Bereiche verbinden könnten.

3.2. Web Authentication API (WebAuthn) und FIDO2/Passkeys

3.2.1. Überblick und Standardisierungsstatus

Die Web Authentication API (WebAuthn) ist eine W3C Recommendation, die eine API für Webanwendungen definiert, um Public-Key-Credentials für starke Authentifizierung zu erstellen und zu verwenden [10]. WebAuthn Level 1 und Level 2 sind Recommendations. Die Arbeit an Level 3 verfeinert weiterhin die Fähigkeiten und verbessert die Abstimmung mit FIDO2 und Passkey-Einsätzen.

WebAuthn arbeitet zusammen mit dem von der FIDO Alliance definierten Client to Authenticator Protocol (CTAP). Gemeinsam bilden sie FIDO2 und decken sowohl die Schnittstelle zwischen Browser und Authenticator (CTAP) als auch die API der Webanwendung (WebAuthn) ab.

3.2.2. Sicherheitseigenschaften

WebAuthn-Credentials haben mehrere wichtige Eigenschaften:

- Origin-Bindung: Credentials sind an einen bestimmten RP-Identifier gebunden, was Phishing und Wiederverwendung verhindert.
- Public-Key-basiert: Der Server speichert Public Keys. Private Keys verlassen den Authenticator nie. Dadurch wird der Authenticator zu einem Faktor, der für Ein- oder Mehr-Faktor-Authentifizierung geeignet ist.
- Attestation: Authenticatoren können Attestation Statements bereitstellen, mit denen RPs (und eID-Schemata) die Sicherheitseigenschaften des Authenticators beurteilen können.
- Phishing-Resistenz: WebAuthn ist darauf ausgelegt, klassische Phishing-Angriffe zu neutralisieren, indem die Authentifizierung an die im Browser angezeigte Origin gebunden wird [10].

FIDO2-Authenticatoren können Plattform-Authenticatoren (in Geräte eingebaut) oder Roaming-Authenticatoren (zum Beispiel USB- oder NFC-Token) sein. CTAP 2.2 standardisiert darüber hinaus Hybrid-Abläufe, bei denen ein Mobilgerät mithilfe von QR-Codes und Nähe-Kanälen wie Bluetooth als Authenticator für einen Desktop-Browser dient [11].

3.2.3. Aktueller Einsatz im eGovernment

In Österreich unterstützt ID Austria bereits FIDO2-Token mit WebAuthn als alternativen zweiten Authentifizierungsfaktor. Der zuständige Infrastrukturbetreiber A-Trust führt FIDO-Token als unterstützt für die Auslösung von ID Austria an, mit der Voraussetzung, dass sie FIDO2-Level-2-zertifiziert sind und WebAuthn unterstützen [18].

Diese Integration zeigt, dass eID-Schemata mit hohem Vertrauensniveau WebAuthn oder FIDO2 als Teil ihrer Mehr-Faktor-Authentifizierungsketten einbinden können, im Einklang mit den Anforderungen der eIDAS-Vertrauensniveaus.

3.2.4. Rolle unter eIDAS

Unter eIDAS 2 und dem EUDI-Wallet-Rahmen spielen WebAuthn und FIDO2 zwei Rollen:

1. Authentifizierung gegenüber RPs: Wie bei eIDAS 2 können Relying Parties WebAuthn oder Passkeys direkt als Faktor für das Bürger:innen-Login verwenden, auch für Portale der öffentlichen Verwaltung, sofern das Gesamtschema die regulatorischen Anforderungen an das Vertrauensniveau erfüllt.
2. Sichere Remote-Wallet-Abläufe: EUDI ARF Topic F beschreibt Remote-Abläufe auf demselben Gerät und geräteübergreifend, bei denen der Browser über das Internet mit einer Wallet interagiert und die Nähe beim geräteübergreifenden Ablauf durch CTAP-2.2-Hybrid-Abläufe (QR-Code und ein Nähe-Kanal wie Bluetooth) abgesichert wird [6,15].

3.3. Digital Credentials API (DC API)

3.3.1. Überblick und Standardisierungsstatus

Die Digital-Credentials-Spezifikation definiert die Digital Credentials API als Web-API, die es User Agents ermöglicht, die Präsentation und Ausstellung digitaler Nachweise zu vermitteln [3]. Die API erweitert Credential Management Level 1 und führt einen Credential-Typ `DigitalCredential` ein. RP-Websites können:

- Credentials von User Agents anfordern (über `navigator.credentials.get()` mit Digital-Credential-Optionen)
- Credentials mithilfe von Ausstellungsoperationen erstellen oder speichern

Die Spezifikation wird von der W3C Federated Identity Working Group entwickelt und wurde als Working Draft auf dem Recommendation-Track veröffentlicht [3,11,16].

Die DC-API-Spezifikation betont, dass die API protokollunabhängig ist und auf einer von der Working Group verwalteten Registry unterstützter Protokolle beruht. Die DC API unterliegt außerdem einer gründlichen Datenschutz- und Sicherheitsprüfung, da sie hochsensible Informationen offenlegen kann [3,6].

3.3.2. Implementierungen in Browsern und Plattformen

Die Implementierungsunterstützung ist rasch vorangeschritten:

- Chrome: Ein Origin Trial für die Digital Credentials API begann mit Chrome 128 und führte seitdem zur allgemeinen Verfügbarkeit ab Chrome 141, sodass Websites Nutzerinformationen mithilfe digitaler Ausweise datenschutzfreundlich überprüfen können [12,13,21].
- Safari: Die Entwicklerdokumentation von Apple beschreibt, wie Safari die Digital Credentials API nutzt, um mobile Dokumente (ISO bzw. IEC 18013 5 oder 7 mdocs) von Apps auf dem Gerät anzufordern, und vermerkt, dass dabei die W3C Digital Credentials API, ISO-Standards für Anfrageformate und FIDO CTAP für plattformübergreifende Abläufe verwendet werden [14].
- Android: Der Credential Manager von Android stellt eine DigitalCredential-API bereit, die OpenID4VP und OpenID4VCI für Präsentation und Ausstellung gegenüber Wallet-Apps unterstützt [25].

Ein Überblick aus 2025 hält fest, dass sowohl Chrome als auch Safari inzwischen die Digital Credentials API unterstützen, wobei sich der genaue Funktionsumfang zwischen den Plattformen unterscheidet [24].

3.3.3. Integration mit VC und OID4VCI bzw. OID4VP

Die Digital Credentials API ist als Transportschicht für übergeordnete Credential-Protokolle und -Formate konzipiert. Das EUDI ARF und verwandte Dokumentation sehen vor, dass:

- Credentials grundsätzlich dem Verifiable Credentials (VC) Data Model v2.0 entsprechen [7]
- Ausstellungs- und Präsentationsabläufe OID4VCI und OID4VP als OAuth-basierte APIs verwenden

Die Spezifikation OpenID for Verifiable Presentations definiert ausdrücklich einen Modus, in dem OID4VP-Nachrichten anstelle von HTTPS-Redirects über die Digital Credentials API übertragen werden [9]. Dadurch kann die Kommunikation zwischen Wallet und RP über Protokollnachrichten laufen, die über die DC API des Browsers ausgetauscht werden, wobei Wallet und Browser sich über das Betriebssystem abstimmen.

3.3.4. DC API in der EUDI Wallet und unter eIDAS 2

Das Discussion Topic F des EUDI ARF, Digital Credentials API, beschreibt die DC API als mögliche Plattform-API für Remote-Transaktionsabläufe [6,15].

Wesentliche Punkte sind:

- Abläufe auf demselben Gerät: Browser und Wallet laufen auf demselben Gerät. Die DC API ruft die Wallet über vom Betriebssystem bereitgestellte Schnittstellen auf.
- Geräteübergreifende Abläufe: Browser und Wallet befinden sich auf verschiedenen Geräten, aber in räumlicher Nähe. Die DC API wird mit CTAP-2.2-Hybrid-Abläufen (QR-Code und ein Nähe-Kanal) kombiniert, um die Interaktion abzusichern.
- Souveränität der Wallet: Die Wallet bleibt für Zustimmung der Nutzenden, Auswahl der Credentials und Durchsetzung von Richtlinien verantwortlich. Der Browser fungiert als Transport- und Vermittlungsschicht, nicht als IdP.
- Umfang: Die aktuelle Arbeit konzentriert sich auf die Präsentation. Die Ausstellung von Attestierungen liegt für die erste Version ausdrücklich außerhalb des Umfangs, kann aber in künftigen Aktualisierungen berücksichtigt werden [6].

Faktisch stellt die DC API die Webstandard-Verbindung zwischen EUDI-Wallets und Web-Relying-Parties dar.

3.3.5. Reifegrad und offene Fragen

Obwohl die Digital Credentials API rasch vorangeschritten ist, vom Entwurf über Origin Trials bis zum Einsatz in großen Browsern, werden mehrere Fragen weiterhin diskutiert:

- Governance der Protokoll-Registry: welche Protokolle und Formate registriert werden sollen, wie eine Diskriminierung zwischen Credential-Formaten vermieden werden kann und wie EU-Durchführungsrechtsakte berücksichtigt werden
- Datenschutzrisiken: Die Spezifikation hält fest, dass die DC API sensible Attribute und Browsing-Verhalten offenlegen kann. Gegenmaßnahmen sind strikte Zustimmung der Nutzenden, eingeschränkter Origin-Zugriff und Minimierung verknüpfbarer Identifikatoren [3,6]
- Interoperabilität zwischen Plattform-APIs und Browser-APIs: Die DigitalCredential-API von Android im Credential Manager und plattformspezifische Mechanismen (zum Beispiel zum Anfordern von ISO-mdocs) müssen mit der DC API auf Web-Ebene zusammenarbeiten [14,25]

Aus eGovernment-Sicht ist die Digital Credentials API strategisch zentral, entwickelt sich aber noch weiter.

4. Zuordnung der Webstandards zu eGovernment-Anwendungsfällen

4.1. Repräsentative eGovernment-Anwendungsfälle

Für diese Zuordnung betrachten wir sechs Anwendungsfälle:

- UC1: Nationales Bürger:innen-Login bei Online-Diensten (zum Beispiel Behördenportal Österreich)
- UC2: Grenzüberschreitende Authentifizierung
- UC3: Qualifizierte elektronische Signaturen (QES)
- UC4: Präsentation von Attributen und Credentials (zum Beispiel Berufsberechtigungen, Altersverifikation)
- UC5: Nutzung von eID oder EUDI-Wallets im privaten Sektor (zum Beispiel Banken, Telekommunikation)
- UC6: Szenarien mit hohem Datenschutzbedarf (zum Beispiel Gesundheit, Sozialdienste) mit starken Verknüpfbarkeitsbeschränkungen

4.2. Ausgangslage: OIDC oder SAML

ID Austria bindet Diensteanbieter über OpenID Connect und SAML 2.0 an. Die offizielle Dokumentation listet OIDC-Discovery- und Endpunkt-URLs auf und beschreibt die Nutzung in browserbasierten und nativen App-Szenarien [16,14]. ID Austria bietet außerdem eine qualifizierte elektronische Signatur, die EU-weit einer handschriftlichen Unterschrift gleichgestellt ist [17,18].

In diesem Aufbau gilt:

- UC1 und UC5 werden gut unterstützt (Login im nationalen und privaten Sektor)
- UC2 wird über die eIDAS-Föderationsarchitektur unterstützt
- UC3 wird durch die Kopplung der ID-Austria-Authentifizierung an QES-Dienste bei Vertrauensdiensteanbietern realisiert [19]
- UC4 ist auf Attribute beschränkt, die in Assertions des ID-Austria-Systems enthalten sind
- UC6 hängt eher von betrieblichen Richtlinien als von technischen Mechanismen ab

4.3. FedCM

Für UC1 (nationales Login) und UC5 (Login im privaten Sektor) kann FedCM als browservermitteltes Front-End für die OIDC-Endpunkte von ID Austria dienen:

- Die RP integriert FedCM. Der Browser nutzt die OIDC-Konfiguration von ID Austria, um mit dem IdP zu interagieren, und zeigt einen nativen Dialog „Mit ID Austria anmelden".

- Das verbessert die Benutzererfahrung und beseitigt die Abhängigkeit von Third-Party-Cookies, im Einklang mit den Bemühungen um Tracking-Schutz [22].

Für UC2 (grenzüberschreitend) in einem IdP-zentrierten Szenario (vor der flächendeckenden Einführung der EUDI-Wallet) könnte FedCM ebenfalls als Front-End für ausländische nationale IdPs dienen, die an eIDAS-Nodes angebunden sind.

In Szenarien mit hohem Datenschutzbedarf (UC6) sind die Datenschutzeigenschaften von FedCM besser als bei klassischem SSO, bleiben aber durch die Sichtbarkeit für den IdP begrenzt. Die Kombination von FedCM mit datenschutzfördernden Protokollen wie BISON könnte das Tracking weiter verringern, erfordert aber zusätzlichen Standardisierungs- und Implementierungsaufwand [19,20].

4.4. WebAuthn und FIDO2/Passkeys

WebAuthn/FIDO2 wird in ID Austria bereits als zweiter Faktor verwendet und unterstützt damit UC1 und UC3 direkt. FIDO2-Level-2-Token mit WebAuthn werden als zusätzlicher Faktor zur Auslösung von ID Austria akzeptiert [18].

Die resultierende Authentifizierung kann zur Autorisierung von QES-Vorgängen verwendet werden, die dann von qualifizierten Vertrauensdiensten ausgeführt werden [17,19].

Für UC2 (grenzüberschreitend) kann WebAuthn Teil des Authentifizierungs-Stacks für notifizierte eID-Schemata sein, sofern deren Vertrauensniveau-Profile die zugrunde liegenden Authenticatoren anerkennen.

Für UC4 (Attributpräsentation) transportiert WebAuthn selbst keine Attribute.

In UC6 (hoher Datenschutzbedarf) begrenzen die origin-gebundenen, Public-Key-basierten Credentials von WebAuthn die RP-übergreifende Verknüpfbarkeit und bieten starke Phishing-Resistenz, was für sensible eGovernment-Dienste vorteilhaft ist.

4.5. Digital Credentials API und Wallet-basierte Abläufe

Die Digital Credentials API ist zentral für künftige Wallet-basierte eGovernment-Interaktionen:

- Für UC1 und UC2 können sich Bürger:innen authentifizieren, indem sie Identitäts-Credentials (zum Beispiel Person Identification Data) aus ihrer EUDI-Wallet über die DC API an RP-Websites präsentieren, mittels OID4VP über die DC API [6,9,15].
- Für UC3 (QES) sieht der EUDI-Rahmen Wallet-basierte Signaturen und qualifizierte Fernsignatur-Erstellungseinheiten (rQSCDs) vor. Die DC API kann die Protokollnachrichten transportieren, die nötig sind, um die Signatursitzung an die RP und den Browser zu binden, wenngleich detaillierte Durchführungsrechtsakte noch entwickelt werden.
- Für UC4 (Attributpräsentation) ist die DC API ausdrücklich darauf ausgelegt, die selektive Offenlegung von Attributen aus Credentials zu unterstützen, wobei geräteübergreifende Abläufe durch CTAP-2.2-Hybrid-Mechanismen abgesichert werden [6,15].
- Für UC5 (Nachnutzung im privaten Sektor) sieht das EUDI ARF Wallet-basierte Interaktionen mit Banken, Telekommunikationsanbietern und anderen privaten Relying Parties vor, wiederum unter Verwendung von Webstandards wie VC 2.0, OID4VCI bzw. OID4VP und DC API [6,15].

In UC6 (hoher Datenschutzbedarf) unterstützt das protokollunabhängige Design der DC API in Kombination mit VC 2.0 und datenschutzfördernden Credential-Formaten wie SD JWT VC minimale Offenlegung und nutzergesteuerte Zustimmung [7]. Das Datenschutzrisiko bleibt, dass leistungsfähige Wallets und Browser-

bzw. Betriebssystemplattformen zur Überwachung missbraucht werden könnten. Der EUDI-Rahmen versucht, dies durch Governance und technische Einschränkungen abzumildern.

5. Diskussion

5.1. Designabwägungen bei browserzentrierter Identität

Der Übergang von Ad-hoc-Abläufen zu browserzentrierten Identitäts-APIs verteilt Verantwortlichkeiten neu. Browser werden zu aktiven Vermittlern sowohl bei der föderierten Anmeldung (FedCM) als auch bei der Wallet-basierten Präsentation von Credentials (DC API). Identity Provider und Wallets müssen sich über standardisierte Endpunkte und Protokolle in diese APIs integrieren. Relying Parties hängen direkter von der Web-Plattform ab.

Das hat mehrere Folgen:

- Sicherheit: Browservermittelte Abläufe können Phishing- und Clickjacking-Risiken verringern und eine bessere Integration mit Authenticatoren auf Betriebssystemebene ermöglichen.
- Datenschutz: Durch die Kontrolle der Oberfläche und die Partitionierung des Zustands können Browser Tracking begrenzen, erhalten aber auch mehr Einblick in Identitätsabläufe, der begrenzt werden muss.
- Interoperabilität: Standardisierte APIs können die Fragmentierung verringern, aber auch neue Lock-in-Vektoren schaffen, wenn nur eine Teilmenge der Browser oder Plattformen sie übernimmt oder wenn bestimmte Wallet-Anbieter dominieren.

Für öffentliche Verwaltungen bedeutet das, dass Entscheidungen von Browser- und Betriebssystemherstellern die Machbarkeit und Zuverlässigkeit nationaler eID- und EUDI-Wallet-Lösungen unmittelbar beeinflussen.

5.2. Sicherheits- und Datenschutzlücken und Forschungsrichtungen

Trotz erheblicher Fortschritte bleiben mehrere Lücken:

IdP-zentrierte versus Wallet-zentrierte Modelle: FedCM verbessert IdP-zentriertes SSO, beseitigt aber das IdP-Tracking nicht. Wallet-zentrierte Modelle mit DC API und VC 2.0 können die Kontrolle stärker zu den Nutzenden verlagern, erfordern aber eine komplexere Infrastruktur und Governance.

Kryptografische Datenschutzverbesserungen: Forschung wie BISON zeigt, dass sich RP-spezifische Pseudonyme so ableiten lassen, dass die Identität der RP vor dem IdP verborgen bleibt [19]. Ähnliche Ideen könnten in künftigen Erweiterungen von OIDC und FedCM standardisiert werden.

Sichere geräteübergreifende Abläufe: Hybride WebAuthn-Abläufe und DC-API-basierte geräteübergreifende Präsentationen verringern Phishing- und Relay-Risiken erheblich, doch reale Einsätze erfordern sorgfältiges Benutzererfahrungs-Design und Bedrohungsmodellierung, besonders wenn Bürger:innen mehrere Geräte und Wallets nutzen.

Transparenz und Governance: EUDI ARF Topic F betont, dass Wallets souverän bleiben müssen. Browser und Betriebssysteme sollten Wallet-Entscheidungen nicht stillschweigend übergehen oder Informationen über die Nutzung von Credentials preisgeben [6]. Dies in der Praxis sicherzustellen, erfordert sowohl technische Mittel (zum Beispiel APIs mit klaren Zustimmungs- und Richtlinien-Hooks) als auch regulatorische Aufsicht.

Post-Quanten-Aspekte werden derzeit nicht berücksichtigt und erfordern weitere Forschung. [2]

5.3. Folgen für öffentliche Verwaltungen

Für öffentliche Verwaltungen bedeuten die analysierten Webstandards eine stufenweise Entwicklung.

Kurzfristig:

- Bestehende OIDC- oder SAML-Einsätze durch WebAuthn bzw. FIDO2 als starke Authentifizierungsfaktoren verbessern, wie es ID Austria bereits tut.
- FedCM für wichtige nationale IdPs in Betracht ziehen, um die Benutzererfahrung und die Widerstandsfähigkeit gegenüber Änderungen beim Tracking-Schutz zu verbessern.

Mittelfristig (EUDI-Rollout):

- Nationale Wallet-Implementierungen und ID-Schemata an VC 2.0, OID4VCI bzw. OID4VP und die Digital Credentials API anpassen, im Einklang mit dem EUDI ARF.[2]
- Remote-Abläufe (auf demselben Gerät und geräteübergreifend) für Anwendungsfälle mit hohem Wert pilotieren, einschließlich grenzüberschreitendem Zugriff und Attributpräsentation.

Langfristig:

- Datenschutzfördernde Erweiterungen (zum Beispiel BISON-artige Pseudonymisierung, Credentials mit minimaler Offenlegung, fortgeschrittene Kryptografie) und Governance-Mechanismen erkunden, die Wallet-Neutralität und Plattform-Rechenschaftspflicht sicherstellen.
- Die Koexistenz mehrerer Modelle (IdP-zentriertes SSO, Wallet-zentrierte Identität, sektorspezifische Schemata) einplanen und Interoperabilitätsprofile definieren.
- Den Übergang zur Post-Quanten-Kryptografie einplanen.

Öffentliche Verwaltungen müssen außerdem in Tests und Konformität investieren: Es muss sichergestellt werden, dass Webanwendungen, Wallets und Browser diese Standards korrekt implementieren und dass Änderungen im Browserverhalten eGovernment-Dienste nicht unbemerkt verschlechtern.

6. Fazit

Browserintegrierte Identitäts-APIs verändern, wie Identität im Web verwaltet wird. FedCM und WebAuthn/FIDO2 sind ausgereift genug, um heute eingesetzt zu werden und Sicherheit, Benutzerfreundlichkeit und Datenschutz nationaler eID-Systeme, einschließlich eGovernment-Diensten, zu

verbessern. FedCM bietet eine browservermittelte Alternative zu klassischem Redirect-basiertem SSO, während WebAuthn phishing-resistente Authentifizierung untermauert und in Kombination mit zertifizierten Authenticatoren hohe Anforderungen an das Vertrauensniveau erfüllen kann.

Die Digital Credentials API entwickelt sich zusammen mit Verifiable Credentials 2.0 und OpenID for Verifiable Credentials (OID4VCI bzw. OID4VP) zum zentralen Webstandard-Stack für Wallet-basierte Identität unter eIDAS 2. Sie bietet eine universell einsetzbare Schnittstelle zwischen EUDI-Wallets und Web-Relying-Parties und ermöglicht die Remote-Präsentation von Identitäts- und Attribut-Credentials sowohl auf demselben Gerät als auch geräteübergreifend.

Das Wallet-basierte Ökosystem entwickelt sich jedoch noch. Implementierungen entstehen in Chrome, Safari und Android, und das EUDI Architecture and Reference Framework verfeinert seine Leitlinien weiter. Öffentliche Verwaltungen sollten DC-API-basierte Lösungen daher als strategisch wichtig, kurzfristig aber nicht als alleinige Grundlage betrachten. Eine EU-Förderung der Entwicklung von Open-Source-Plattformen und -Browsern könnte ein Strategiebaustein für Stabilität und europäische Souveränität sein.

Indem nationale eID-Schemata wie ID Austria an identitätsbezogene Webstandards angepasst werden und dabei die Einschränkungen und offenen Fragen berücksichtigt werden, können sich die Mitgliedstaaten darauf vorbereiten, vom europäischen Rahmen für eine digitale Identität zu profitieren und sichere, datenschutzfreundliche digitale Interaktionen für Bürger:innen und Unternehmen zu ermöglichen.

Referenzen

[*] OpenAI. ChatGPT 5 [Large language model] was used to aid research and to edit parts of the text.

[1] W3C, “Federated Credential Management API”, W3C First Public Working Draft, 2023.

[2] MDN Web Docs, “Federated Credential Management (FedCM) API”, 2025.

[3] W3C, “Digital Credentials”, W3C Working Draft, 2025.

[4] W3C FedID Working Group, “Digital Credentials API – GitHub repository”.

[5] European Union, eIDAS 2: “Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework”, Official Journal L 2024/1183, 30 April 2024.

[6] European Digital Identity Cooperation Group, “Topic F – Digital Credentials API (EUDI ARF Discussion Paper)”, 2025.

[7] W3C Verifiable Credentials Working Group, “Verifiable Credentials Data Model v2.0”, W3C Recommendation, 2024.

[8] OpenID Foundation, “OpenID for Verifiable Credential Issuance 1.0”, Final Specification, 2025.

[9] OpenID Foundation, “OpenID for Verifiable Presentations 1.0”, 2025.

[10] W3C, “Web Authentication: An API for accessing Public Key Credentials Level 1”, W3C Recommendation, 2019.

[11] FIDO Alliance, “Client to Authenticator Protocol (CTAP)”, including CTAP 2.2 documentation.

[12] Chrome Developers, “Introducing the Digital Credentials API origin trial”, 2024.

[13] Chrome Developers, “Digital Credentials API: secure and private identity on the web”, 2025.

[14] Apple Developer Documentation, “Requesting a mobile document on the web”, 2025.

[15] Deep summary of EUDI Digital Credentials API architecture, “Digital Credentials API Architecture – eudi.dev”, 2025.

[16] ID Austria, “Anbindung mit OpenID Connect”, ida.gv.at, accessed 2025.

[17] ID Austria or Austrian Federal Chancellery, “Generelle Informationen zur ID Austria”, including QES information, 2025.

[18] A Trust, “FIDO Tokens – Als zweiten Faktor zur Auslösung der ID Austria”, 2025.

[19] J. Heher, S. More, L. Heimberger, “BISON: Blind Identification with Stateless scOped pseudoNyms”, arXiv:2406.01518, 2024.

[20] J. Heher et al., “BISON - GitHub repository”, 2024.

[21] Chrome Platform Status, “Digital Credentials API (presentation support)”, feature 5166035265650688, 2025.

[22] W3C FedID Working Group, “FedCM – GitHub repository”, 2025.

[23] Corbado, “Digital Credentials API (2025): Chrome & Safari Support Live”, 2025.

[24] Android Central, “Google makes it easier to share digital credentials on your Android phone”, describing Android Credential Manager’s support for OpenID4VP or OIDC4VCI, 2025.

[25] Example open source integration, “ID Austria demo – Next.js”, GitHub repository rudgal/id-austria-demo.

---

1. A-SIT hat zuvor eine frühere Version der Digital Credentials API evaluiert: Implementierung und Evaluierung der Digital Credentials API ↩
2. A-SIT arbeitet in den Projekten PREPARED und POSEIDON in diese Richtung. ↩