Security and Privacy challenges of the Digital Credentials API

Simone Onofri (W3C)

W3C AC meeting 2026
Hangzhou, China
20-22 April 2026

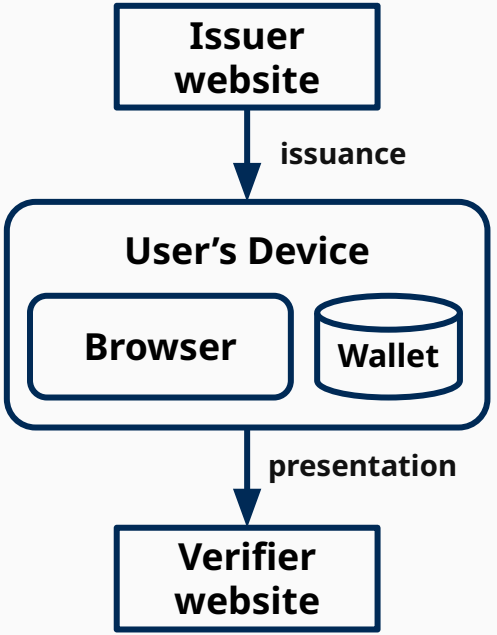
Why a new Web API?

The goal of the **Digital Credentials API** is to **empower users to exchange verifiable credentials securely, privately, and seamlessly on the web.**

It helps users to:

- Understand **what is being requested.**
- **Choose** the **wallet and credential** to use.
- Support **consent**, **interoperability**, and **safe** and **privacy-preserving** patterns.

During the initial chartering phase, **we received a Formal Objection (overruled by the Council)** highlighting the **potential adverse social impact of the identity ecosystem**.



Why I should care about it?

Yes, if your organization develops browsers, platforms, wallets, or works with credentials.

- **Browser and OS platform:** this work defines the Web layer for credential issuance and presentation.
- **Wallet, issuer, and verifiers:** it influences integration expectations, trust boundaries, and interoperability
- **Service Providers and regulated sectors:** such as payments and governments.
- **Users:** it affects disclosure, consent, portability, and exposure to tracking or oversharing.

Examples of external pressure: ***public-sector wallet initiatives such as EUDI Wallet and industry interest in high-trust financial flows.***

What are we working on?

The specification is currently a Working Draft updated on **17 April 2026**, and the **work is active and substantive**.

- We have **91 open issues and 165 closed**; and **8 open PRs and 232 closed**.
- **Security and Privacy continue to be a significant** part of the open work, with 10 open issues for privacy and 7 for security.
- The **current path** still **depends on important discussions and the wide review,** even though **we already have two implementations**.

The realistic timeline is 2026 for wide review and CR preparation, and 2027 for the Recommendation.

What is keeping us busy?

The **main challenges** are still largely about **privacy and security**.

- **Privacy**: oversharing, unlinkability, status checks, and observability across the ecosystem
- **Security**: integrity, misuse, trust assumptions, and malicious adjacent actors
- **Architecture**: distribution of responsibilities across the ecosystem, which includes protocols, wallets, credentials, and trust frameworks

One **source of complexity** is that we are part of the **Decentralized Identity Ecosystem** (including ***protocols***, ***credential*** formats, ***status-check*** algorithms, **wallets**, and ***trust*** frameworks)

What can go wrong?

With the Security Interest Group, we are **working with two complementary threat models**:

- A **higher-level model** covering **security**, **privacy**, and **socio-technical threats**
- A more **specific model focused on the API** and adjacent layers with **14 Threats and 25 Mitigations**.

What are we going to do about it? In a systematic way.

- Which mitigations can we implement within the API, and what residual risks remain?
- How and to what extent to trust, in adjacent layers, e.g., malicious (or compromised) issuers or verifiers.

Threat modeling is helping clarify where safeguards belong: in the Browser and API, or in the wider ecosystem.

What are our open issues?

We have two main issues:

- A **Formal Objection** **has been filed regarding the inclusion of ISO 18013-7 Annex C** because it is **not an Open Standard**.
- More generally, the issue of **interoperability** of the different flows we have - **same-device and cross-device** - across **different platforms** and **protocols**.

Thank you!

Any questions?

simone@w3.org

The point is no longer whether digital identity will reach the Web, but how to protect users without leaving them exposed.