Digital Credential API

The **Digital Credential API** (DCAPI) is a means to sort out queries from a Verifier for the presentation of data from a collection of credentials and direct those queries to a device application that can process the request successfully.

Security

Threats

The Digital Credentials API—designed to let users present data from verifiable credentials (like digital IDs, mDLs or diplomas) directly through their browser raises serious security and privacy concerns. Here are some issues to consider:

1. It's unclear what the criteria are for registering a query language that browsers must accept.
    1. Can an attacker get a bogus language inserted into a browser's list?
2. Overexposure of Personal Data - Websites could request more information than necessary, leading to overcollection or misuse of sensitive credentials. Without strict controls, this opens the door to:
    1. Cross-site tracking based on credential metadata
    2. Fingerprinting users by the types of credentials they hold
3. Browser and Wallet Trust Boundaries - the API involves two user agents: the browser and the digital wallet. If either is compromised or poorly implemented:
    1. Malicious sites might trick users into sharing credentials
    2. Wallets might not clearly show what’s being shared or with whom
4. Lack of User Awareness - even with permission prompts, users may not fully understand:
    1. What data is being requested
    2. Who is requesting it
    3. Whether they can refuse without losing access
    4. This creates a consent theater problem—where users click “Allow” without informed choice.
    5. Does the user know if this request is in-person or on-web? Should they care?
    6. It is not clear who presents what consent request to the user, the device, the browser, the wallet. Could there wind up being 3 consent request UIs?
5. No Universal Mitigation for All Threats
    1. Some threats—like websites inferring identity from credential types—don’t yet have clear technical solutions. Mozilla, for example, has raised formal objections, warning that the API could erode user agency and privacy if not carefully constrained.
6. “The Web Must Never Demand Your Papers”

    1. This principle, echoed by W3C’s Technical Architecture Group, warns against normalizing a web where users must prove identity to access content. If misused, the API could lead to a surveillance-by-default internet.
    2. Phone Home is more of a meme than a specific threat against server retrieval.
7. Registration operation is unclear - will that limit value?
    1. Could a channel (say BLE) be a decentralized self-describing protocol

Mitigations

Some proposed mitigations

- selective disclosure
- trust lists
- wallet-side policy enforcement
- Common UI from in-person and on-web queries