What’s new with Digital Credentials

Lee Campbell - Google

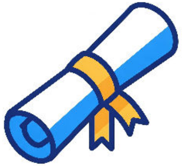
What is a Digital Credential?

Passports

Travel Docs

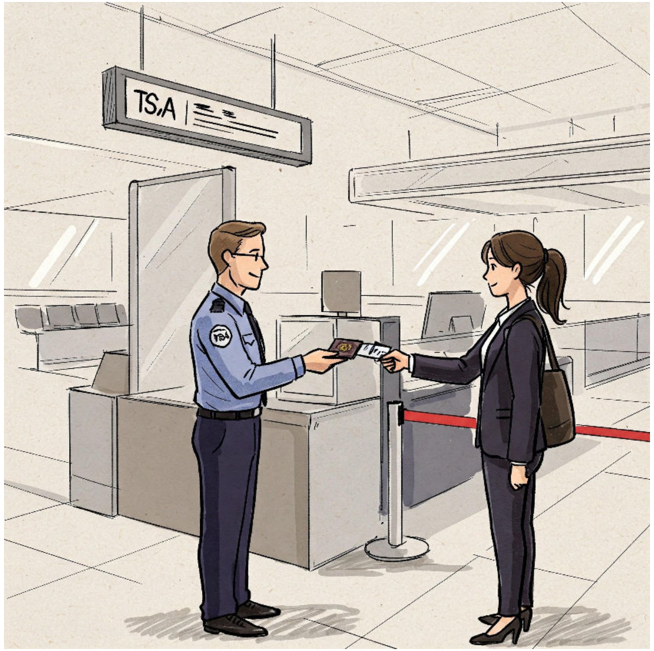
Driving License

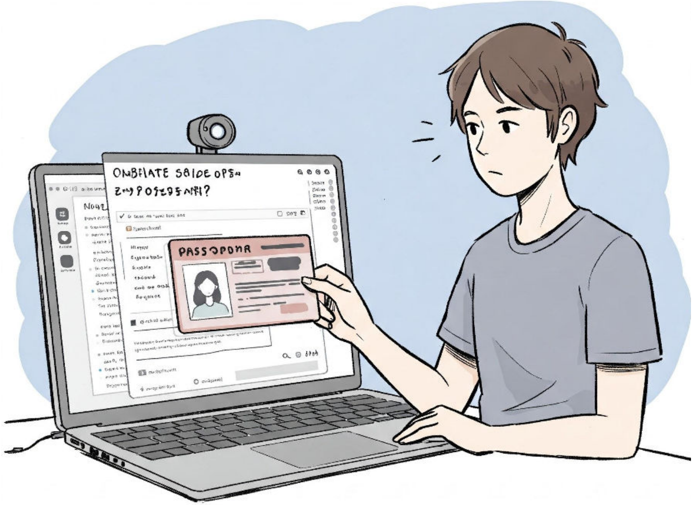
Employee Badges



Diplomas

Digital Credentials can be presented....



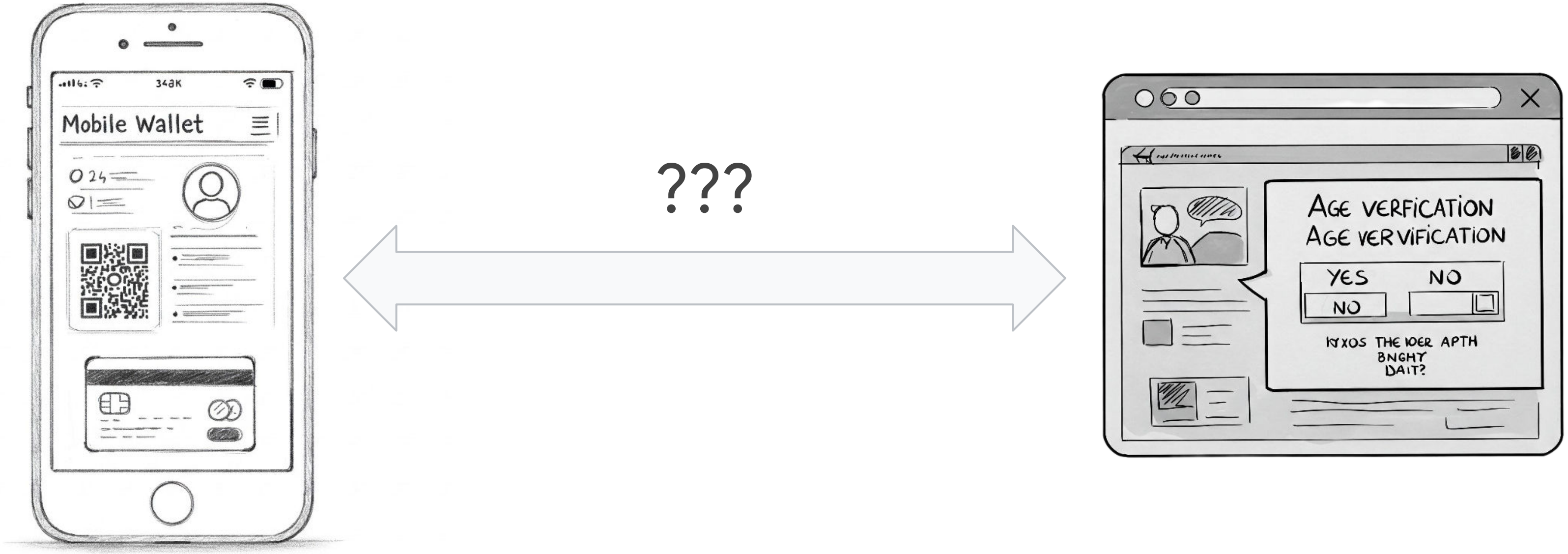


In Person

or

Online

How do websites or apps request Digital Credentials?



???

Requesting a Digital Credential

When a website or app would like to request a Digital Credential it needs to send a Credential Request to the wallet application holding that credential. The wallet processes the request, generates the Credential Response and returns to back to the requester.

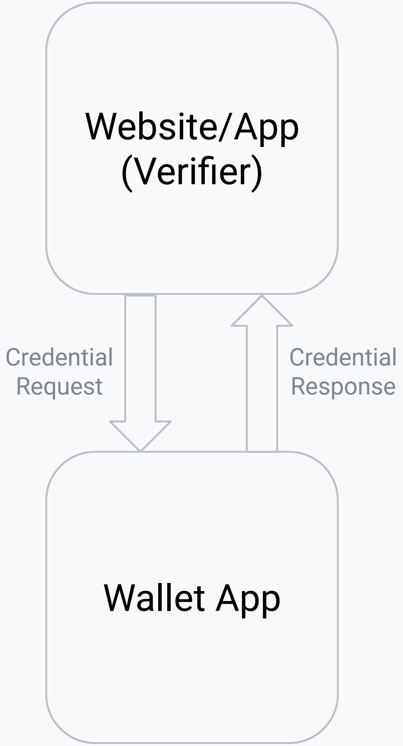
This raises a number of questions:

- How is the Credential Request and Response specified?

OpenID4VP

- How does the Request get to the wallet?
- How does the Response get back to the calling app or website?
- How does the user ensure the Request to routed to the wallet holding the credential they wish to present?
- How does an app or website securely request a credential from a different device?

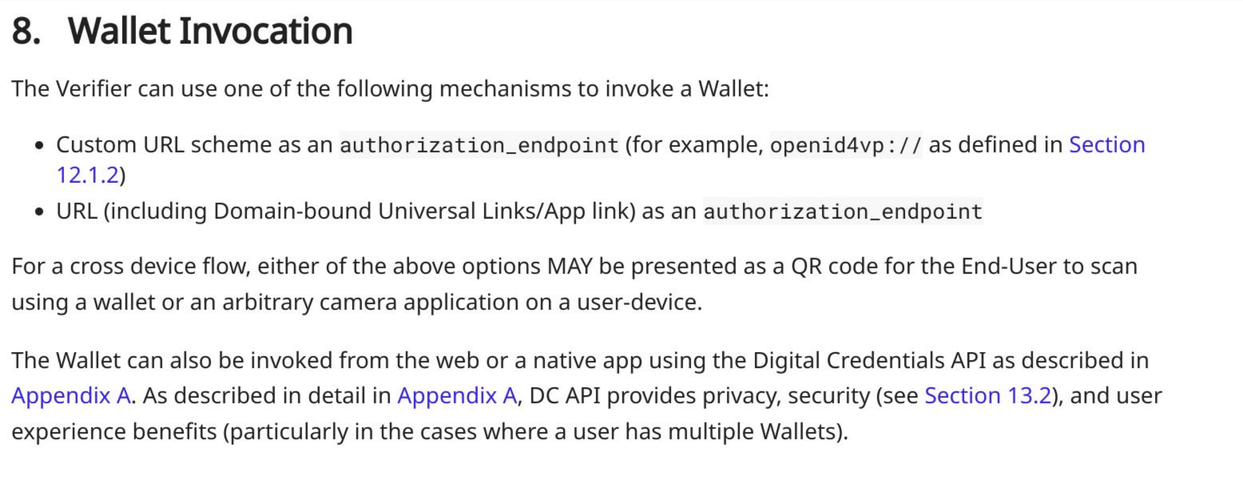
Digital Credentials API



OpenID4VP

OpenID4VP defines the structure of the Credential Request and Response and is mandated by the ARF.

Chapter 8 of the OpenID4VP discusses options for **Wallet Invocation**.



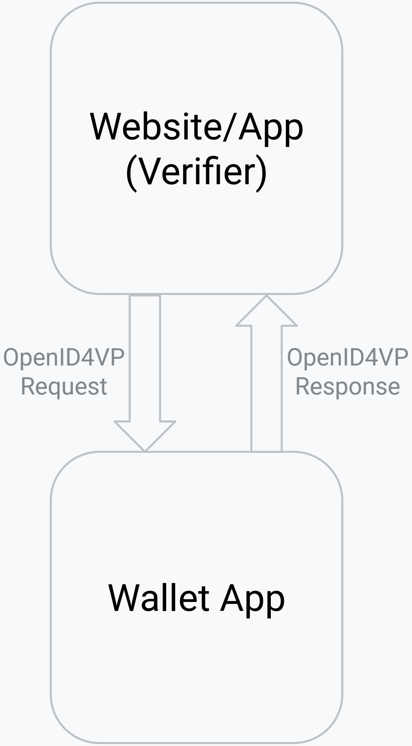
8. Wallet Invocation

The Verifier can use one of the following mechanisms to invoke a Wallet:

- Custom URL scheme as an `authorization_endpoint` (for example, `openid4vp://` as defined in Section 12.1.2)
- URL (including Domain-bound Universal Links/App link) as an `authorization_endpoint`

For a cross device flow, either of the above options MAY be presented as a QR code for the End-User to scan using a wallet or an arbitrary camera application on a user-device.

The Wallet can also be invoked from the web or a native app using the Digital Credentials API as described in Appendix A. As described in detail in Appendix A, DC API provides privacy, security (see Section 13.2), and user experience benefits (particularly in the cases where a user has multiple Wallets).



Wallet Invocation

For an app or website to make a request to the platform it needs to call an API.

When OpenID4VP and the ARF were originally created such an API to request digital credentials didn’t exist, so workarounds had to be found!

The ‘hack’ was to use custom-url schemes, e.g `openid4vp://.....` as a way to pass the request from a website or app to a wallet application. This is really suboptimal for number of reasons and these limitations were well known to the community. For digital wallets to work at scale a solution to this problem needed to be found!

So a group was formed in the W3C to specify a first class wallet invocation API to replace custom-url schemes in OpenID4VP.

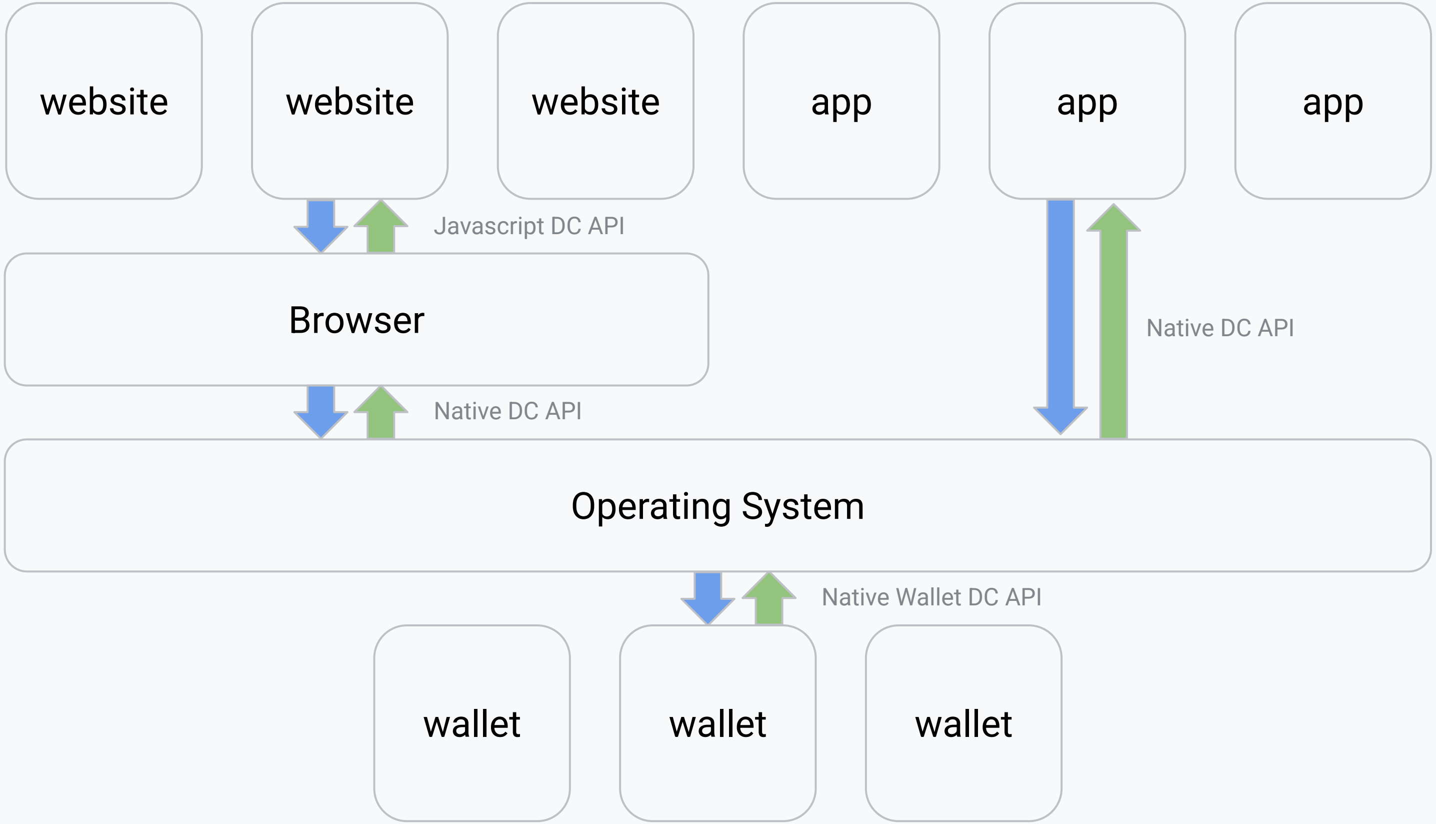
This is the Digital Credentials API

The Digital Credentials API

The API provides a way for a native app or website to request to pass an OpenID4VP request to a mobile wallet application.

- For the web Its defined by the W3C Federated Identity Working Group* as a javascript API
- For native apps, mobile operating systems will provide a native equivalent. For example Android provides the equivalent API for app developers.
- Mobile operating systems also provide an API for wallets to register as credential providers.

Architecture



website

website

website

app

app

app

Javascript DC API

Browser

Native DC API

Native DC API

Operating System

Native Wallet DC API

wallet

wallet

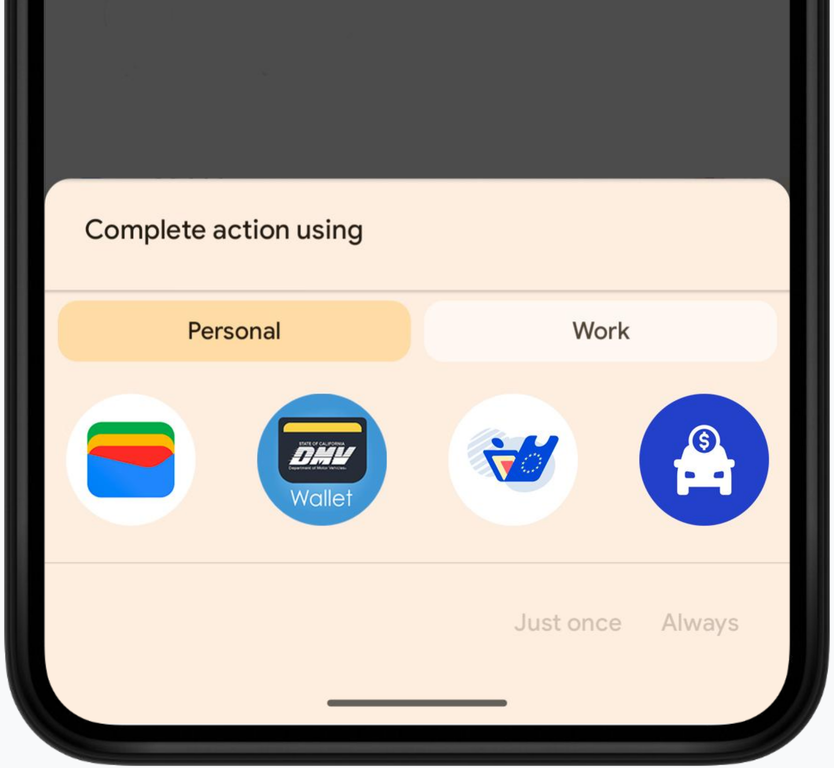
wallet

Credential Selection vs Wallet Selection

We learnt from passkeys that users want to pick the credential to present, not the wallet they may be stored in.

The community believes the user should perform credential selection, not wallet selection during presentation and our UXR confirms this.

This improves credential discovery and allows the user to see exactly what information will be shared if they proceed with a given credential.

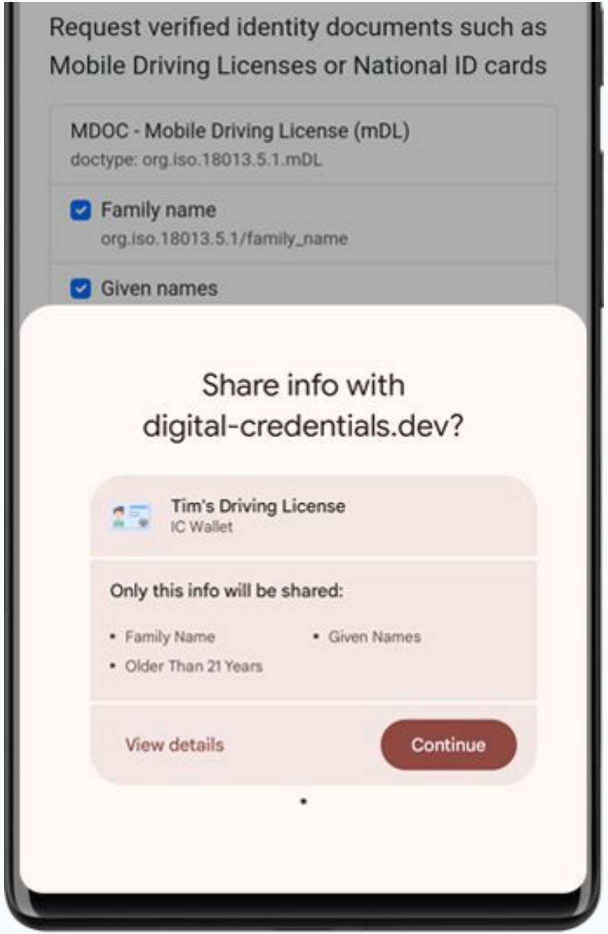


This is poor UX for credential selection.
Users don't recall where a given credential is saved.

Credential Selection vs Wallet Selection

As such, the DC API is designed to run the Credential Request query across all the available wallets and to aggregate the matching credentials into a credential selector.

When the user selects a credential the wallet holding that credential is invoked and takes over the UI.



Request verified identity documents such as Mobile Driving Licenses or National ID cards

MDOC - Mobile Driving License (mDL)
doctype: org.iso.18013.5.1.mDL

☑ Family name
org.iso.18013.5.1/family_name

☑ Given names

Share info with digital-credentials.dev?

Tim's Driving License
IC Wallet

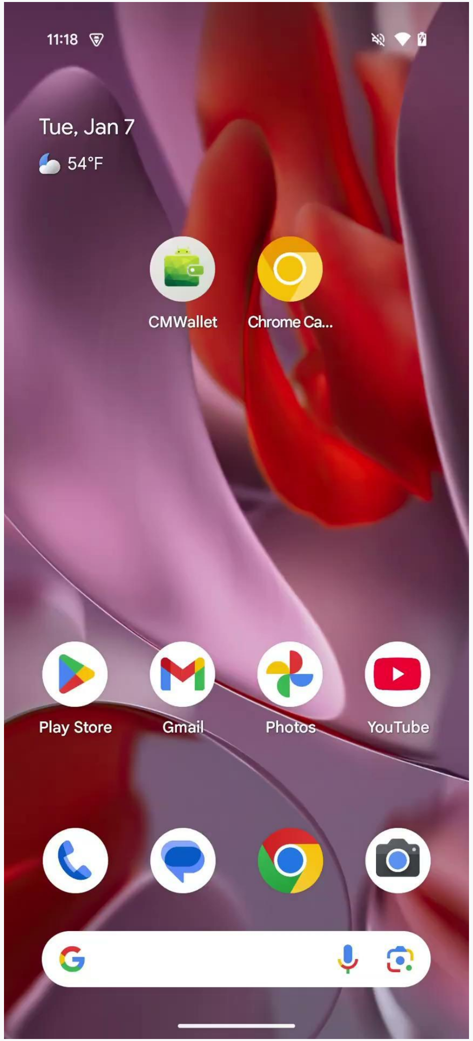
Only this info will be shared:

- Family Name
- Given Names
- Older Than 21 Years

Presentation API

```
let digitalCred = await
  navigator.credentials.get({
       digital: {
         requests: [{
           protocol: "openid4vp",
           data: {
             // OpenID4VP Request
           }
         }]
       }
     });
```

mDL Demo


11:18
Tue, Jan 7
54°F
CMWallet
Chrome Ca...
Play Store
Gmail
Photos
YouTube

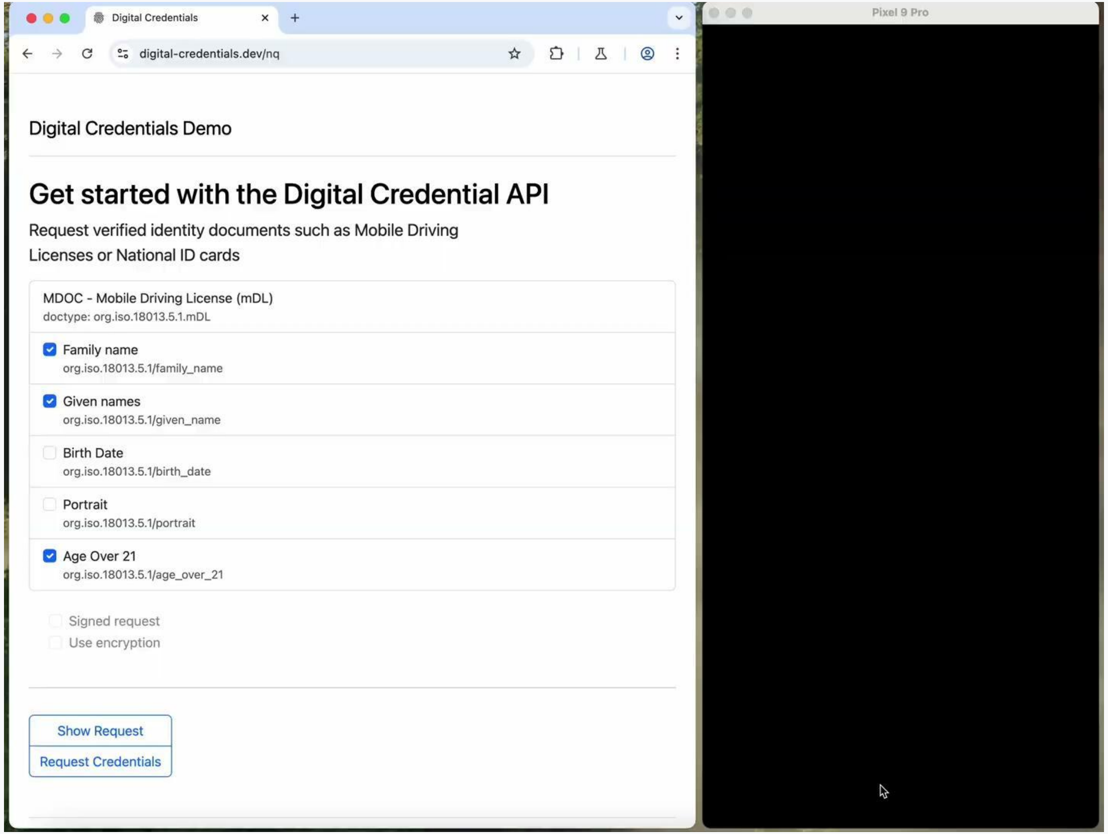
Cross Device

One key advantage of the DC API is seamless and phishing resistant cross device presentation.

Today users are able to present passkeys between devices using a industry standard protocol called CTAP. CTAP is supported by all major operating systems and browsers.

The FIDO Alliance maintains the CTAP specification and the community recently updated this spec to support Digital Credentials.

Cross Device Demo



Digital Credentials Demo

Get started with the Digital Credential API

Request verified identity documents such as Mobile Driving Licenses or National ID cards

MDOC - Mobile Driving License (mDL)
doctype: org.iso.18013.5.1.mDL

- ☑ Family name
  org.iso.18013.5.1/family_name
- ☑ Given names
  org.iso.18013.5.1/given_name
- □ Birth Date
  org.iso.18013.5.1/birth_date
- □ Portrait
  org.iso.18013.5.1/portrait
- ☑ Age Over 21
  org.iso.18013.5.1/age_over_21

□ Signed request
□ Use encryption

Show Request
Request Credentials

DC API Cross Device advantages

- Phishing resistant
- Consistent UX
- No verifier developer overhead
- No wallet developer overhead
- Works across platforms
- Optimized UX for known devices, can skip the QR code
- New transports come for free, e.g UWB
- Supports all features of OpenID4VP (inc Payments)

Issuance

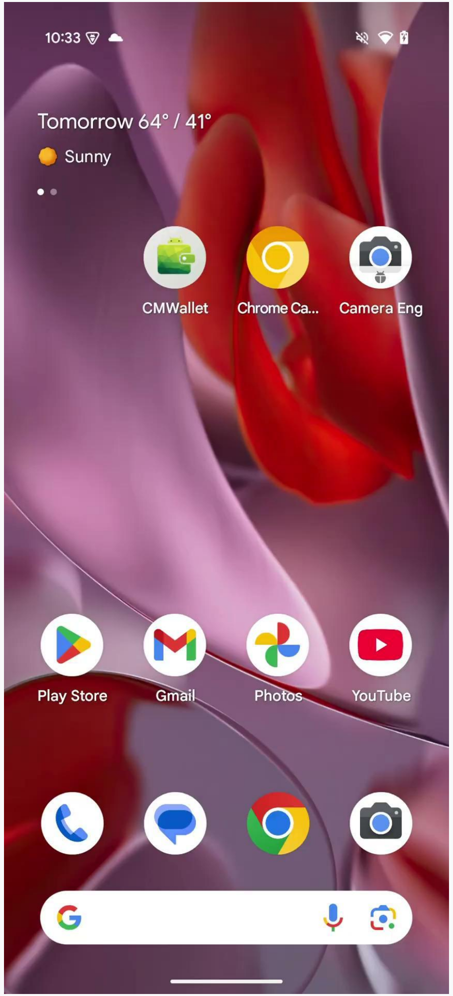
The DC API also have Issuance on the roadmap. This API allows websites and apps to store a credential in a user's wallet

- Currently available in Chrome Canary behind a flag
- Looking to add to the standard Q1'25
- Supports OpenID4VCI
- Also works seamlessly cross device.

Issuance API

```
let result = await
  navigator.credentials.create({
       digital: {
         requests: [{
           protocol: "openid4vci",
           data: {
             // OpenID4VCI Credential Offer
           }
         }]
       }
     });
```

Issuance Demo

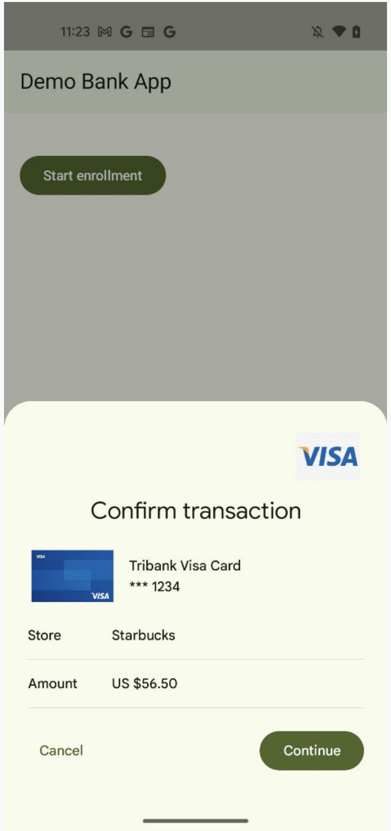


Digital Payment Credentials - DPCs

There is work ongoing in the EU to use Digital Credentials to authenticate and make payments

Given we have a first class API, the platform can provide special UX treatment for different types of credentials and presentations.

For example we can optimize the presentation of a payment credential during payment confirmation.



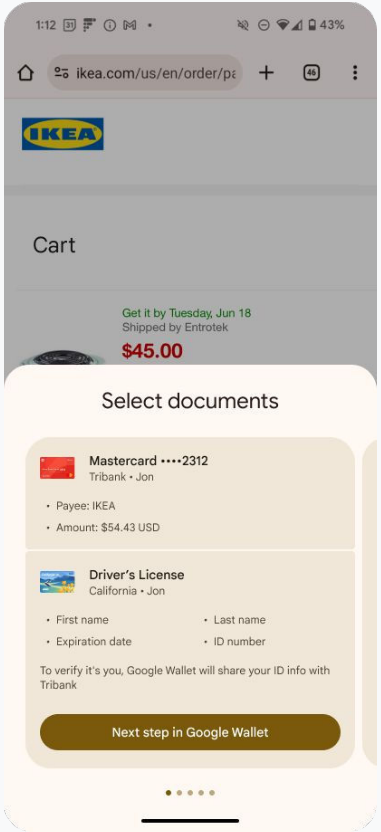
Confirm transaction

Tribank Visa Card
*** 1234

Store	Starbucks
Amount	US $56.50

Combined Presentations

OpenID4VP allows us do combined presentations, such as payment and age verification in a single call.



Cart

Get it by Tuesday, Jun 18
Shipped by Entrotek
$45.00

Select documents

Mastercard ••••2312
Tribank • Jon

- Payee: IKEA
- Amount: $54.43 USD

Driver's License
California • Jon

- First name
- Last name
- Expiration date
- ID number

To verify it's you, Google Wallet will share your ID info with Tribank

Summary

- Digital IDs are here and are rolling out fast
- New Digital Credentials API and OpenID4VP allows websites and apps to request these IDs
- You can try this now!