Digital Credentials API

European Commission

EU Digital Identity Wallet

Lee Campbell

Co-Chair, Digital Credentials WG
@ FIDO Alliance

Tim Cappalli

@ timcappalli.me

Co-Chair, Digital Credentials WG
@ FIDO Alliance

Editor, Digital Credentials API @ W3C

Maintainer, digitalcredentials.dev

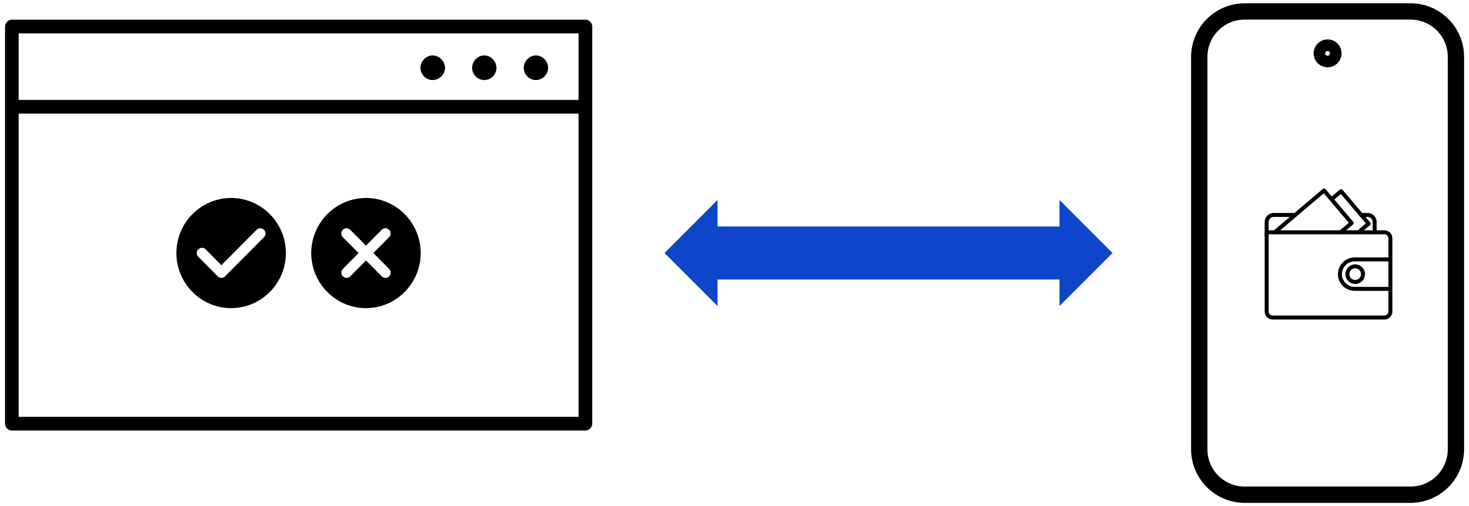
Andreea Stefan

Product Area Lead
@ **ING** Global Platform

(Authentication, ID&V, Approval & Consent)

The Why

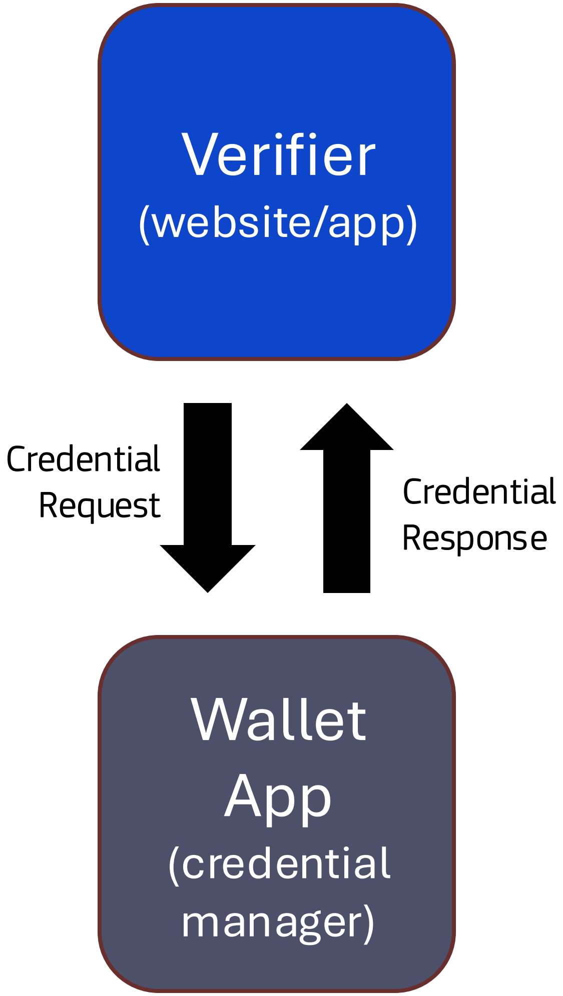
How do websites or apps request Digital Credentials?



Requesting a Digital Credential

When a website or app would like to request a Digital Credential, it needs to:

1. Send a Credential Request to the wallet application holding that credential.
2. The wallet processes the request, generates the Credential Response and returns to back to the requester.



Verifier
(website/app)

Credential Request

Credential Response

Wallet App
(credential manager)

Requesting a Digital Credential

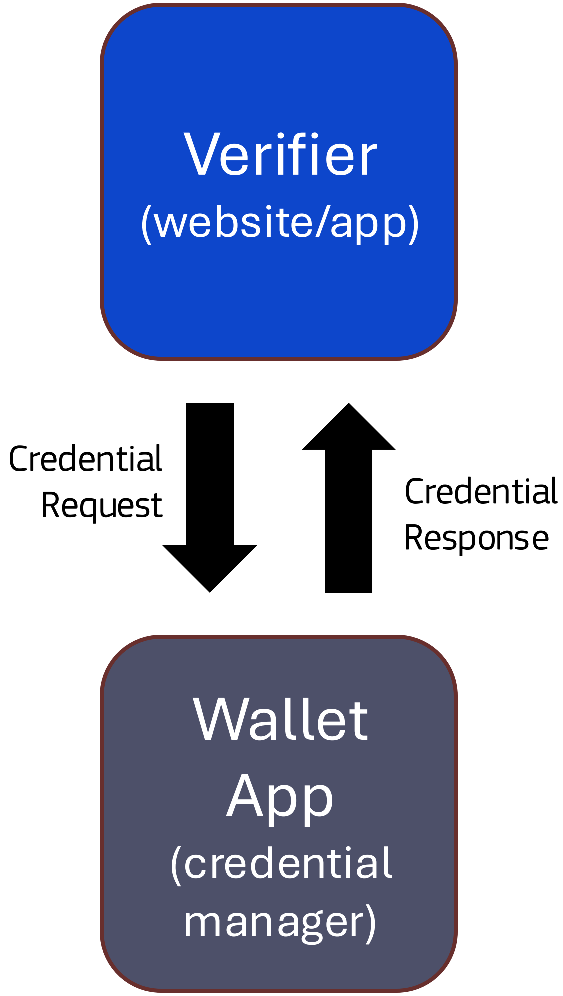
This raises several questions:

OpenID4VP

- How is the Credential Request and Response specified?

- 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 is routed to the wallet holding the credential they wish to request?
- How does an app or website securely request a credential from a different device?

Digital Credentials API



Before the DC API

Custom Schemes

Custom Schemes

A non-standard way to invoke a native app from the web

Typically defined by protocols but any value can be used, by anyone

```
mdoc://
openid4vp://
haip://
eudi-openid4vp://
openid-credential-offer://
+
++
...
```

Best Case

CUSTOM SCHEMES

The user may obtain a viable experience if:

- They have a single wallet app installed
- That wallet has the requested credential provisioned
- The request can be handled by a single wallet
- You are in a browser context that supports schemes

Best Case

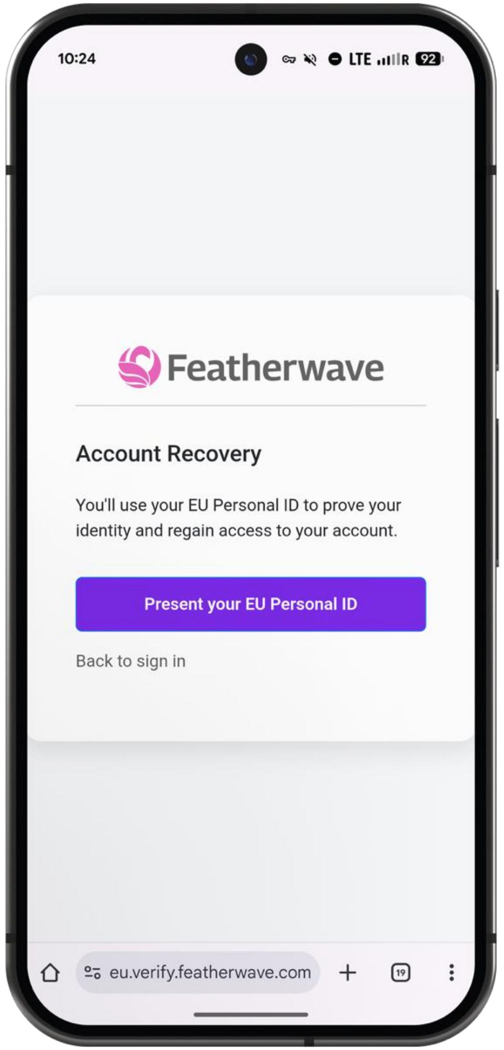
CUSTOM SCHEMES

The user may obtain a viable experience if:

- They have a single wallet app installed
- That wallet has the requested credential provisioned
- The request can be handled by a single wallet
- You are in a browser context that supports schemes

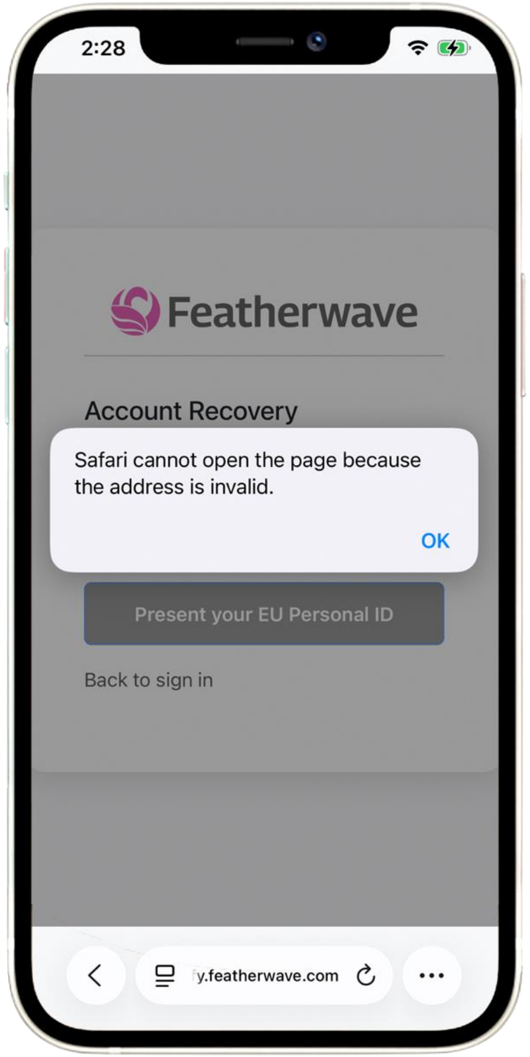
This is the case you test and demonstrate, but the real world is much less forgiving :)

Chrome
on
Android



Account Recovery

You'll use your EU Personal ID to prove your identity and regain access to your account.



Account Recovery

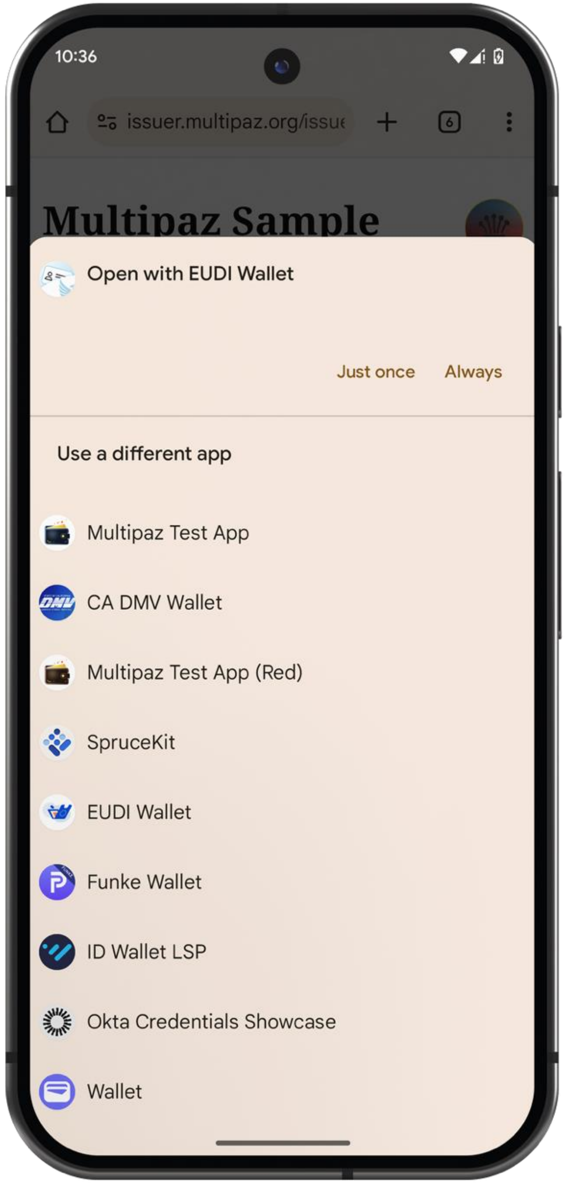
Safari cannot open the page because the address is invalid.

Safari
on
iOS

Android

Multiple apps registered for same custom scheme

Note:
All these apps are shown regardless if they have a relevant credential



10:36

issuer.multipaz.org/issue

Multipaz Sample

Open with EUDI Wallet

Just once Always

Use a different app

- Multipaz Test App
- CA DMV Wallet
- Multipaz Test App (Red)
- SpruceKit
- EUDI Wallet
- Funke Wallet
- ID Wallet LSP
- Okta Credentials Showcase
- Wallet

iOS

Multiple Apps not supported. Behavior undefined.

Other Issues

CUSTOM SCHEMES

- Fragile responses.
  - Redirect URLs are problematic
  - RPs may need to implement arbitrary timeouts

- Browser support/behavior is not assured. It may change over time
  - Expect extra UX friction in all major browsers!
  - Generally, not supported in WebViews at all

Other Issues

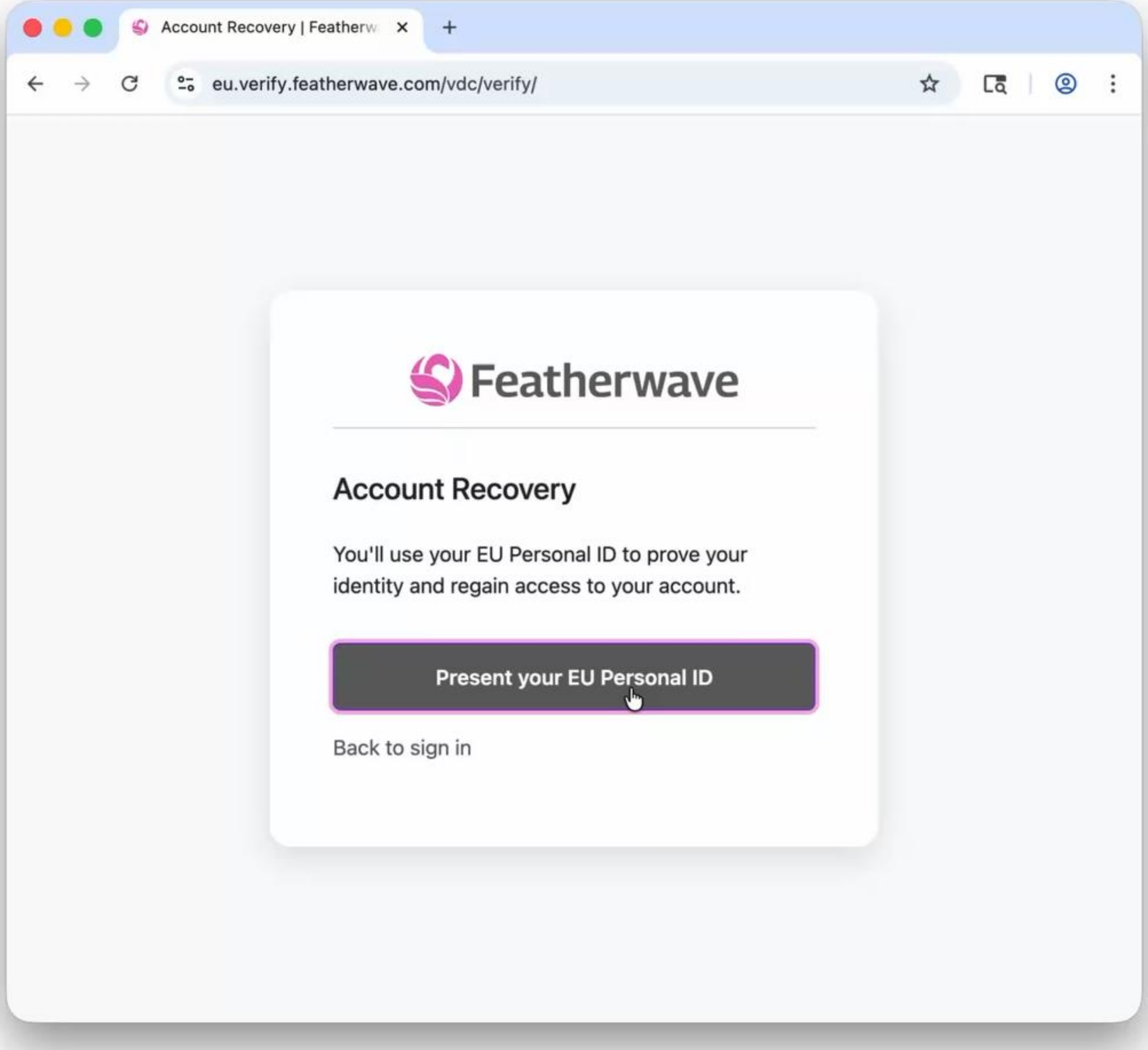
CUSTOM SCHEMES

- No secure source of origin. This causes phishing issues.
- No requirement for a secure context
- Verifiers need to handle cross device as a special case
  - Unclear what to do on tablets
- Payments use-cases will have too high friction for transactions.
- Multi Credentials Requests can't work across wallets
- Not all camera apps handle custom schemes well.

Experience w/ the Digital Credentials API

European Commission | EU Digital Identity Wallet

European Commission | EU Digital Identity Wallet

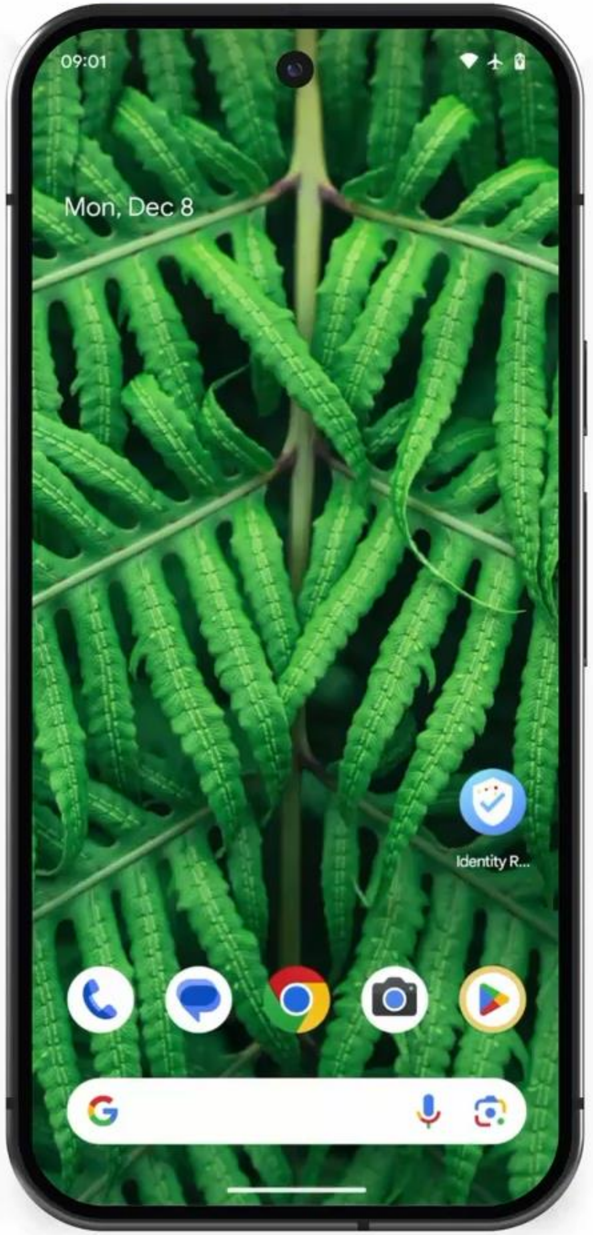


Account Recovery | Featherw
eu.verify.featherwave.com/vdc/verify/
Featherwave

Account Recovery

You'll use your EU Personal ID to prove your identity and regain access to your account.

Present your EU Personal ID
Back to sign in

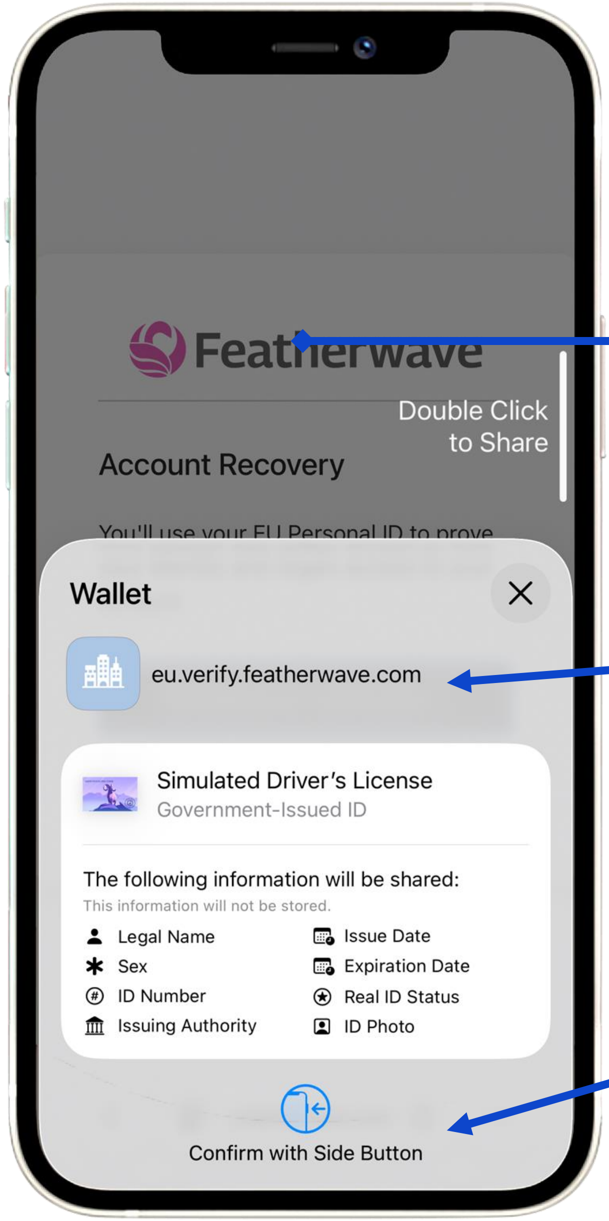


User Experience, Privacy, & Security

European Commission

EU Digital Identity Wallet

Invoked from a secure context



Featherwave

Double Click to Share

Account Recovery

You'll use your EU Personal ID to prove

Wallet

eu.verify.featherwave.com

Simulated Driver's License

Government-Issued ID

The following information will be shared:

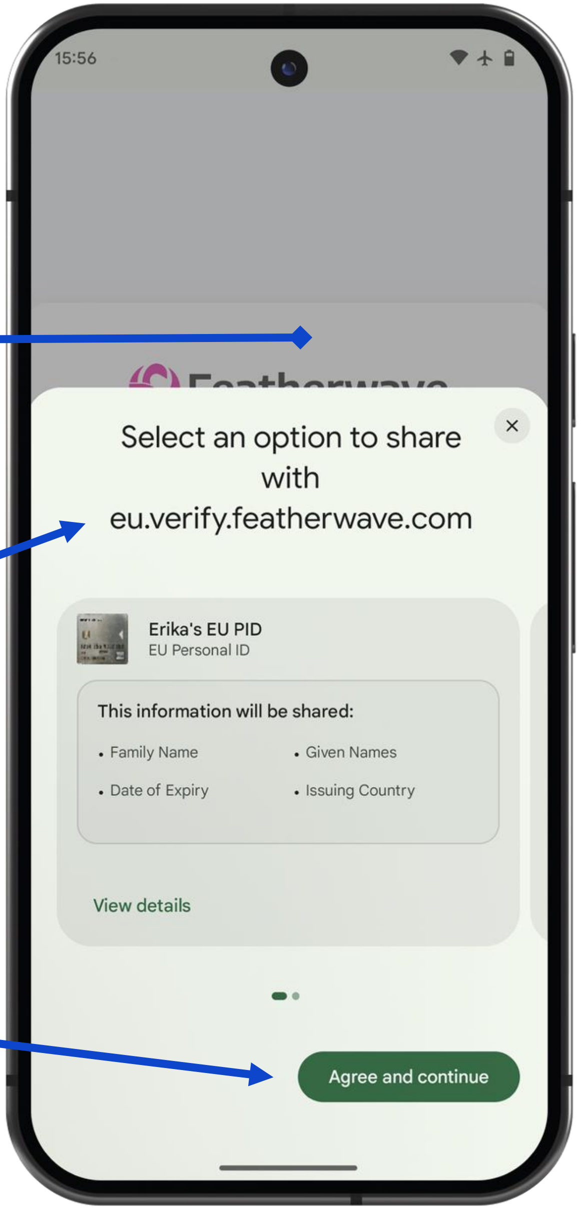
This information will not be stored.

- Legal Name
- Sex
- ID Number
- Issuing Authority
- Issue Date
- Expiration Date
- Real ID Status
- ID Photo

No context switch

Requestor identity

Nothing disclosed to apps until user gives permission



Select an option to share with eu.verify.featherwave.com

Erika's EU PID

EU Personal ID

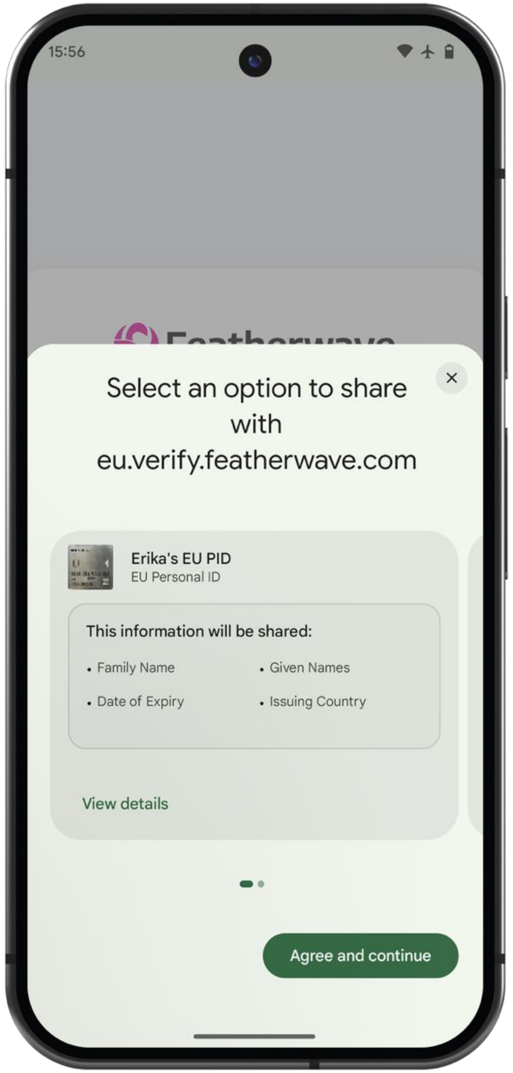
This information will be shared:

- Family Name
- Given Names
- Date of Expiry
- Issuing Country

European Commission | EU Digital Identity Wallet

Credential Selection

- Only provisioned and matching credentials are shown
- Inline provisioning is possible
- Users understand what's going to happen before they share information with a wallet app



15:56

Select an option to share with eu.verify.featherwave.com

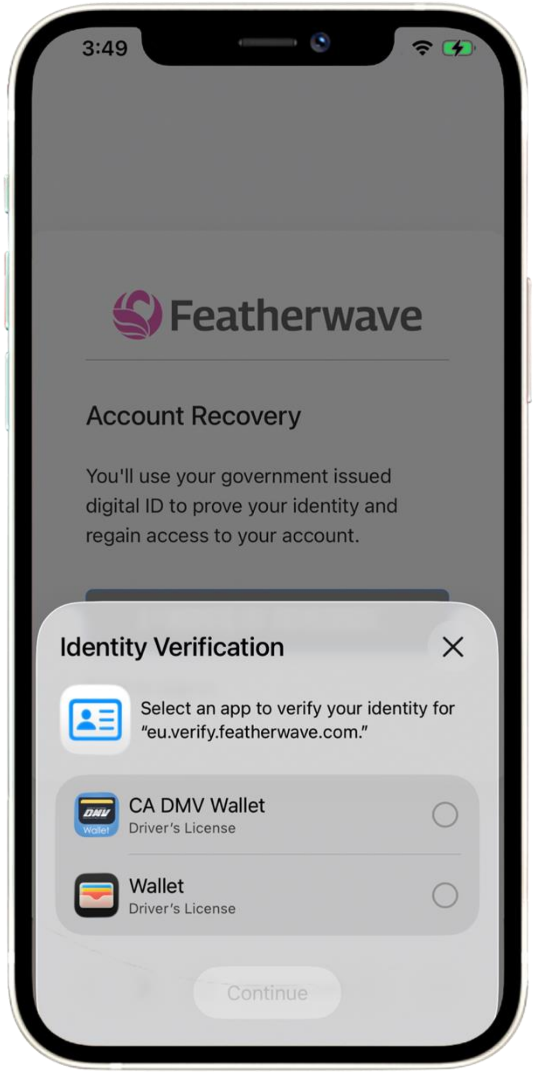
Erika's EU PID
EU Personal ID

This information will be shared:

- Family Name
- Given Names
- Date of Expiry
- Issuing Country

View details

Agree and continue



3:49

Featherwave

Account Recovery

You'll use your government issued digital ID to prove your identity and regain access to your account.

Identity Verification

Select an app to verify your identity for "eu.verify.featherwave.com."

CA DMV Wallet ○
Driver's License

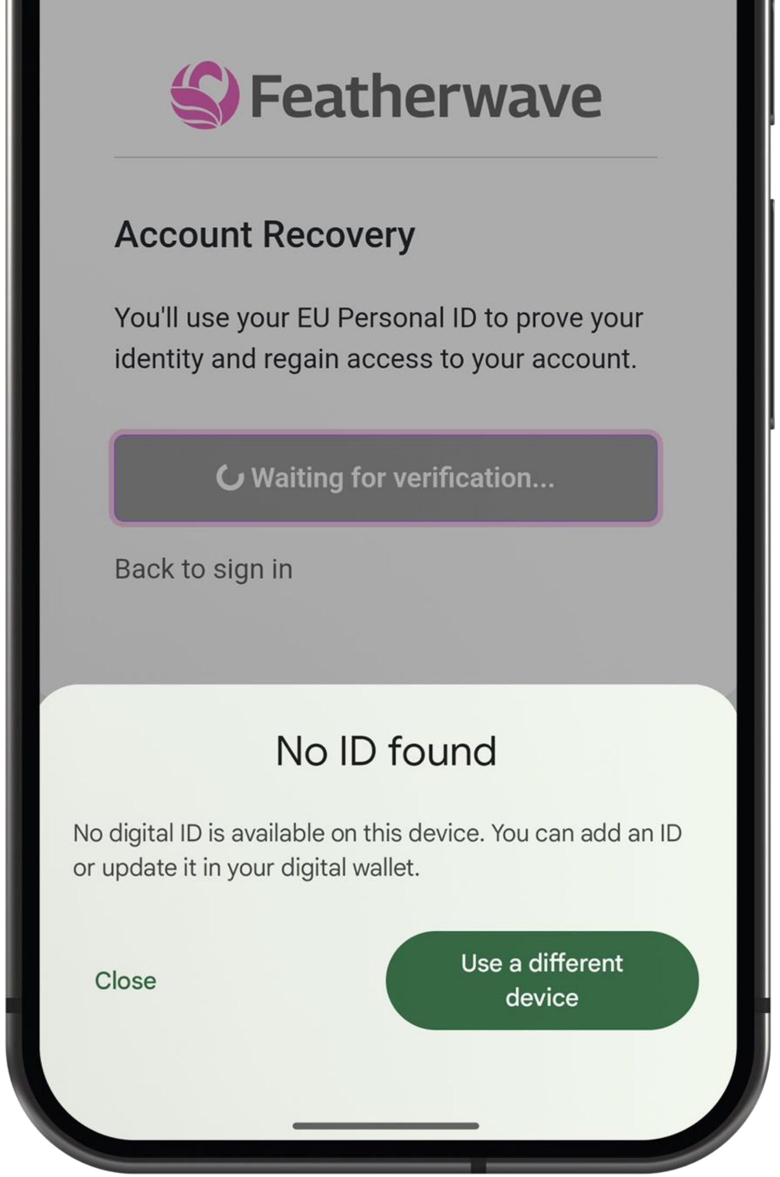
Wallet ○
Driver's License

Continue

European Commission | EU Digital Identity Wallet

No Credentials

- No credentials handled gracefully and deterministically on all platforms.
- Both for no wallets installed and for no matching credentials
- Seamless cross device fallback



Featherwave

Account Recovery

You'll use your EU Personal ID to prove your identity and regain access to your account.

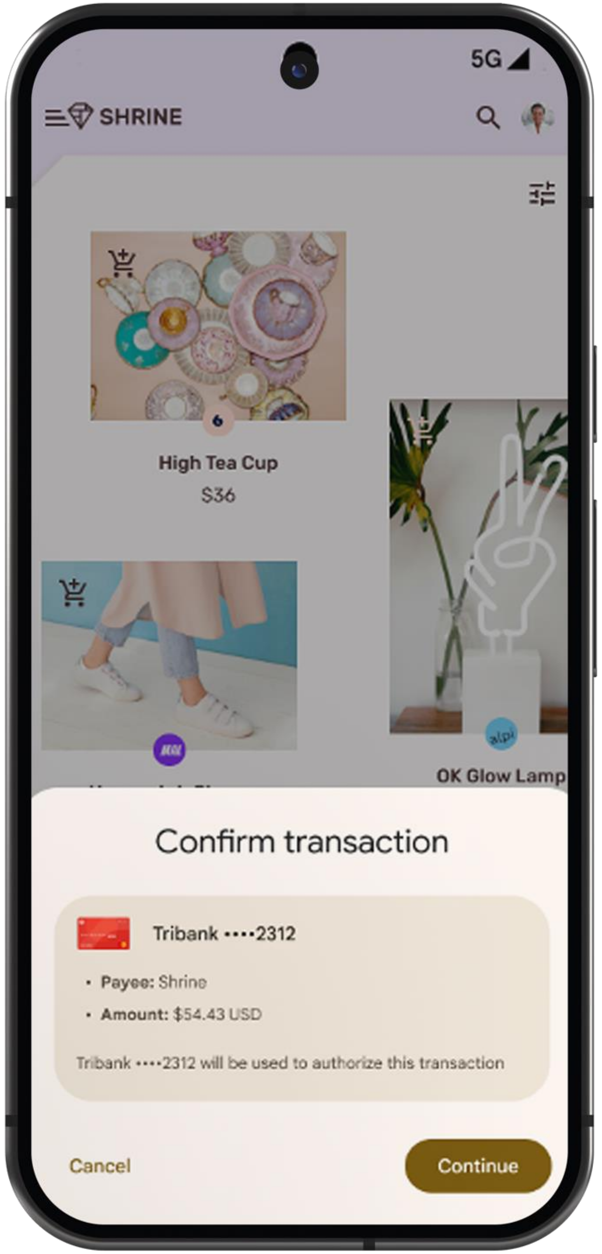
No ID found

No digital ID is available on this device. You can add an ID or update it in your digital wallet.

European Commission | EU Digital Identity Wallet

Optimized UX
Complex Use-Cases

- Optimized UX for Payments
- Multi Credential Presentations

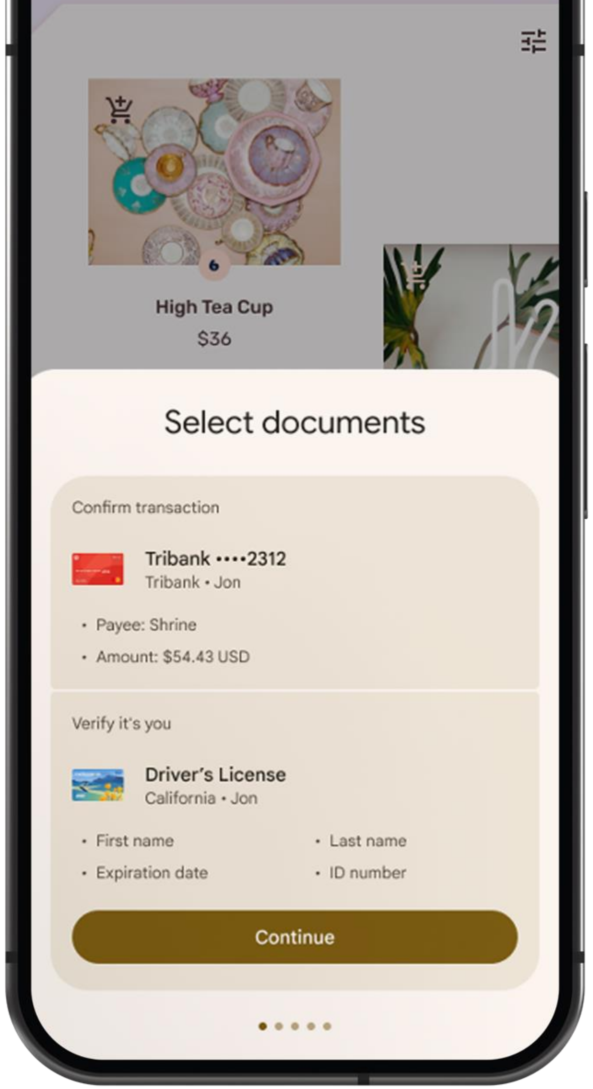


Confirm transaction

Tribank ••••2312

- **Payee:** Shrine
- **Amount:** $54.43 USD

Tribank ••••2312 will be used to authorize this transaction



Select documents

Confirm transaction

Tribank ••••2312
Tribank • Jon

- Payee: Shrine
- Amount: $54.43 USD

Verify it's you

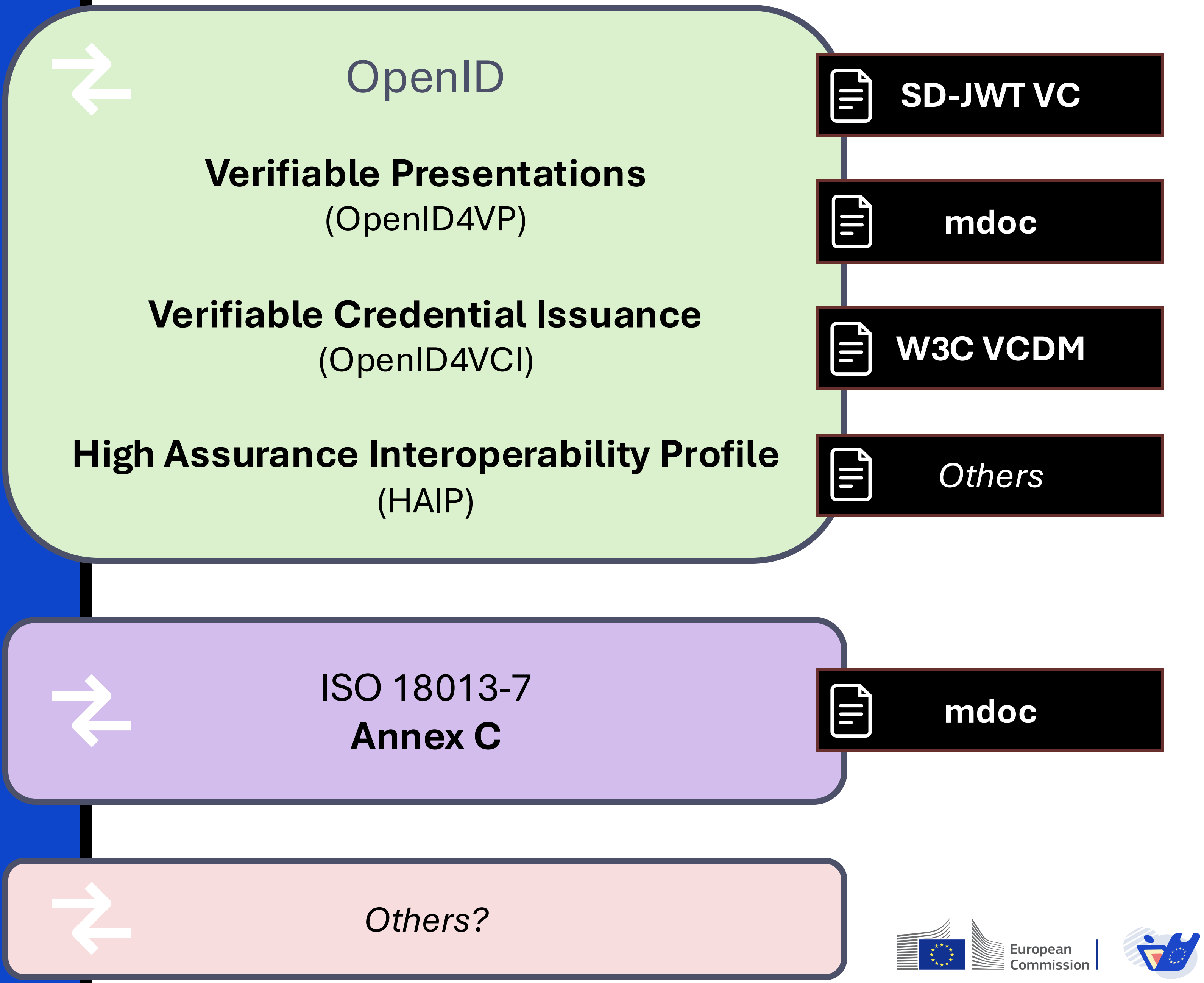
Driver's License
California • Jon

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

European Commission | EU Digital Identity Wallet

How It Works

W3C **Digital Credentials API**



OpenID

Verifiable Presentations
(OpenID4VP)

Verifiable Credential Issuance
(OpenID4VCI)

High Assurance Interoperability Profile
(HAIP)

SD-JWT VC

mdoc

W3C VCDM

Others

ISO 18013-7
Annex C

mdoc

Others?

Presentation

```
let presentation = await navigator.credentials.get({
  digital: {
    requests: [
      {
        protocol: "openid4vp-v1-signed",
        data: { // OpenID4VP Request }
      },
      {
        protocol: ”org-iso-mdoc",
        data: { // 18013-7 Annex C Request }
      }
    ]
  }
});
```

Presentation

```
let presentation = await navigator.credentials.get({
  digital: {
    requests: [
      {
        protocol: "openid4vp-v1-signed",
        data: { // OpenID4VP Request }
      },
      {
        protocol: ”org-iso-mdoc",
        data: { // 18013-7 Annex C Request }
      }
    ]
  }
});
```

Same request via multiple protocols

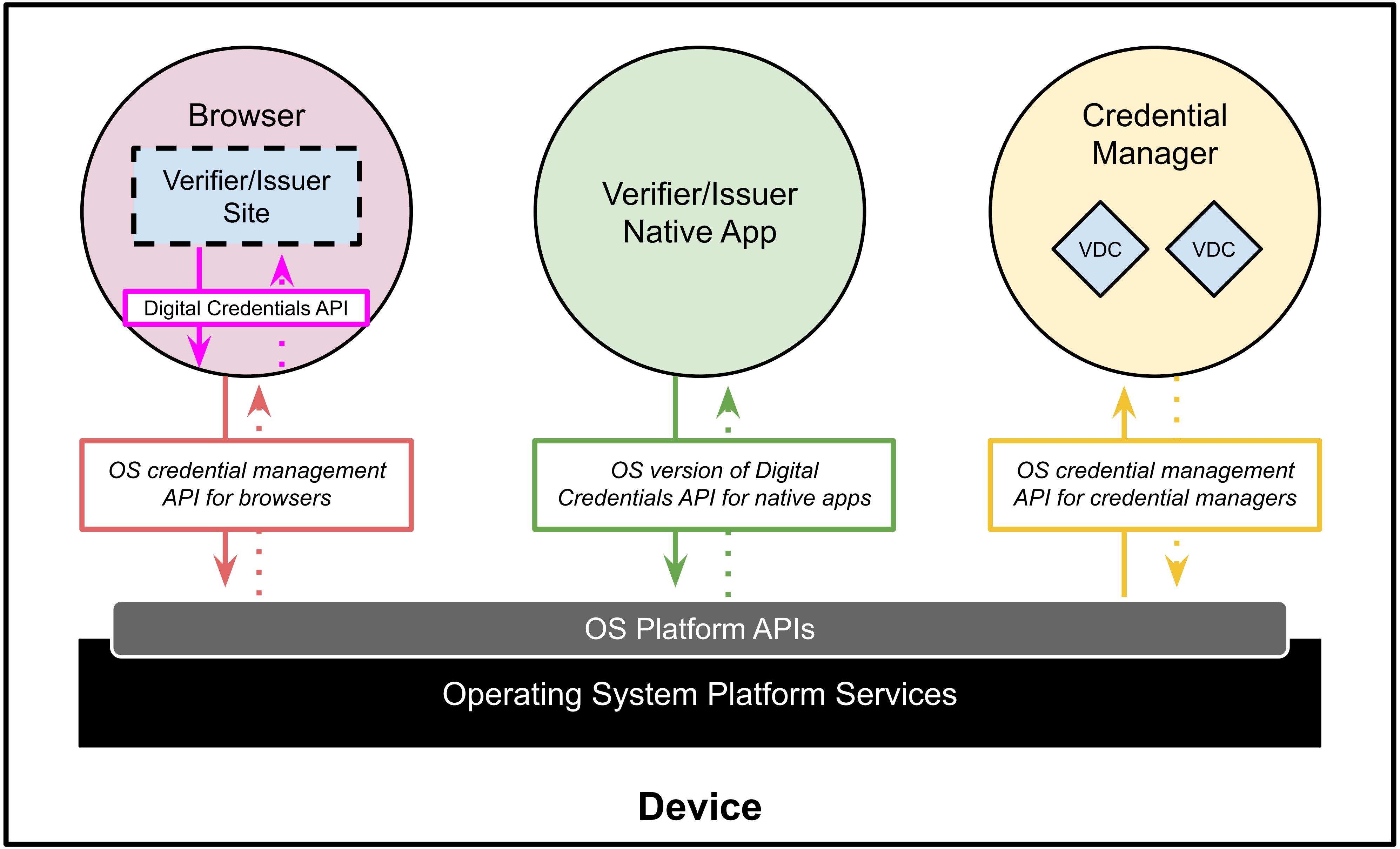
Issuance

```
let presentation = await navigator.credentials.create({
  digital: {
    requests: [
      {
        protocol: "openid4vci-v1",
        data: { // OpenID4VCI Request }
      },
      {
        protocol: "openid4vci-v2",
        data: { // OpenID4VCI v2 Request }
      }
    ]
  }
});
```

Issuance

```
let presentation = await navigator.credentials.create({
  digital: {
    requests: [
      {
        protocol: "openid4vci-v1",
        data: { // OpenID4VCI Request }
      },
      {
        protocol: "openid4vci-v2",
        data: { // OpenID4VCI v2 Request }
      }
    ]
  }
});
```

Protocol agility


Browser
Verifier/Issuer Site
Digital Credentials API
Verifier/Issuer Native App
Credential Manager
VDC
VDC
OS credential management API for browsers
OS version of Digital Credentials API for native apps
OS credential management API for credential managers
OS Platform APIs
Operating System Platform Services
Device

Seamless Cross-Device

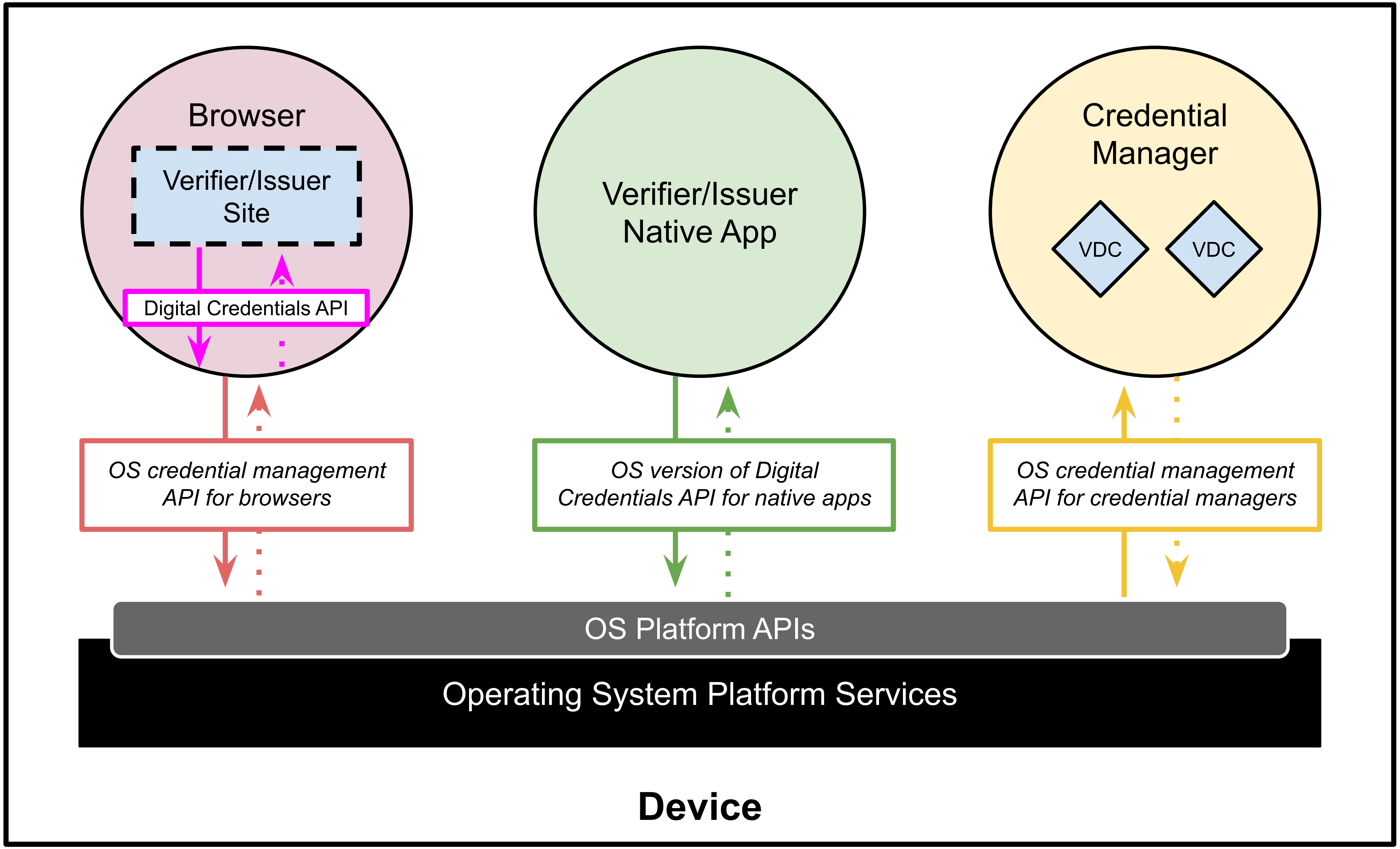
European Commission

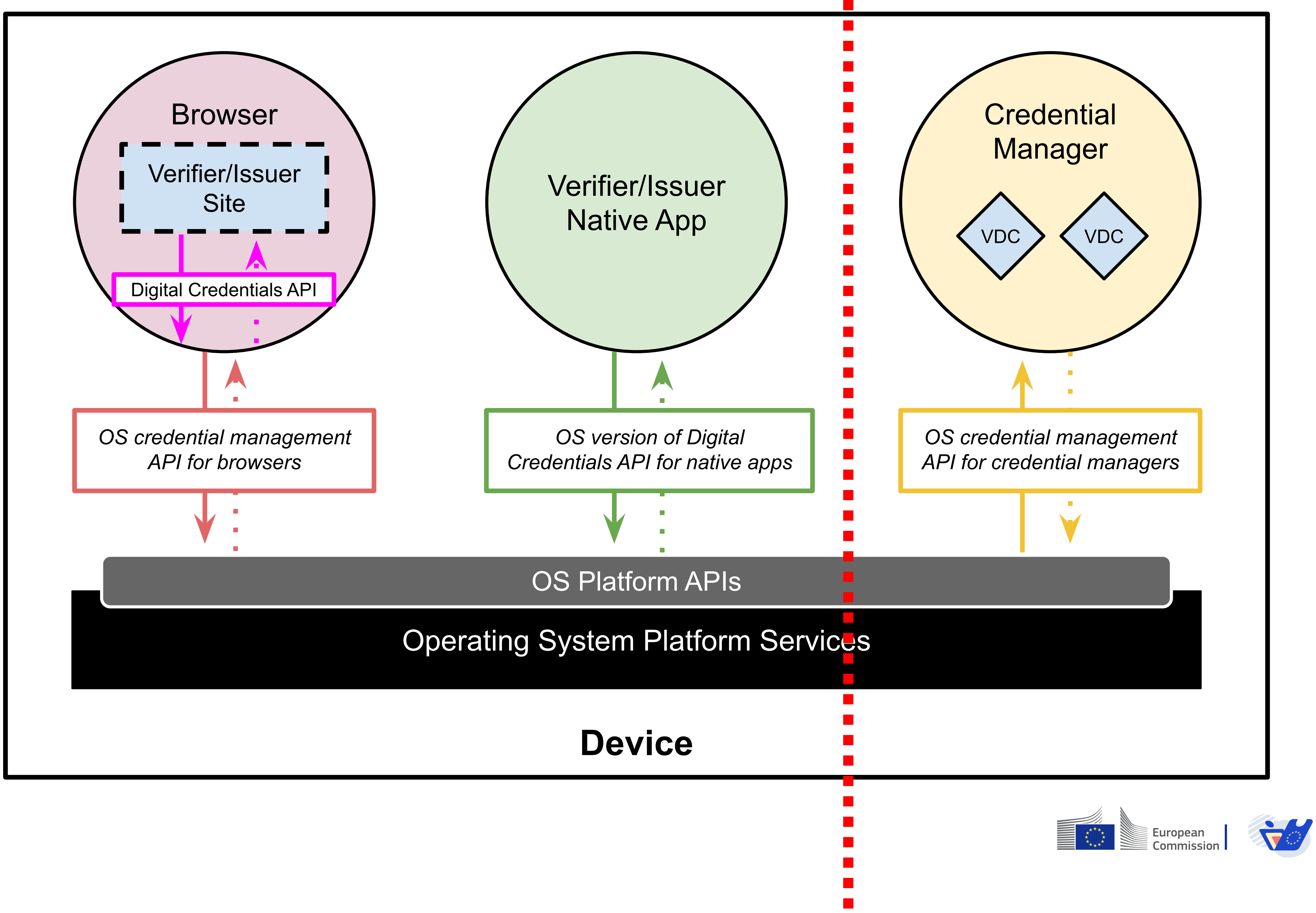
EU Digital Identity Wallet

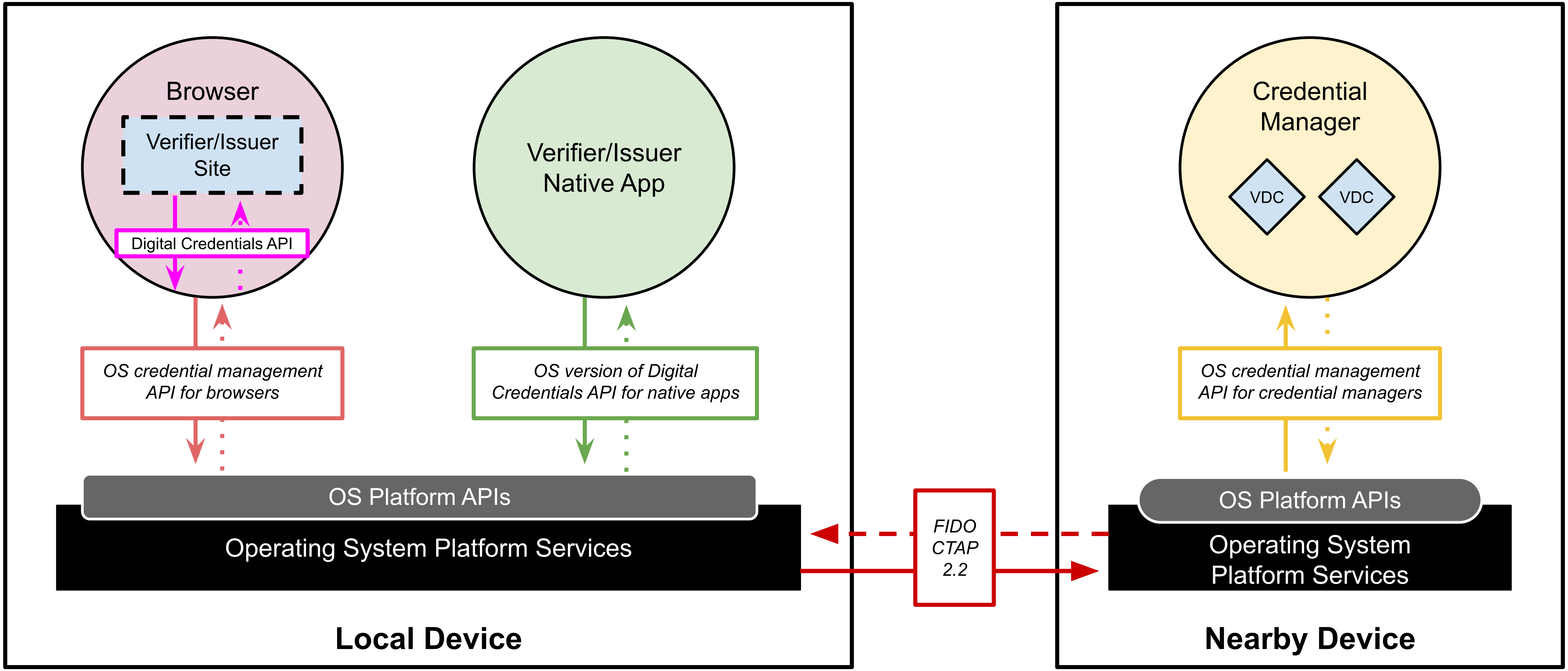
Seamless Cross-Device

- Phishing resistant
- Consistent user experience
- Works across platforms
- No verifier/issuer developer overhead
- No wallet developer overhead

- UX optimized for known devices (skip QR code)
- New/additional transports come for free
(ex: Ultra-wideband)
- Supports all features of presentation and issuance protocols


Browser
Verifier/Issuer Site
Digital Credentials API
Verifier/Issuer Native App
Credential Manager
VDC
VDC
OS credential management API for browsers
OS version of Digital Credentials API for native apps
OS credential management API for credential managers
OS Platform APIs
Operating System Platform Services
Device


Browser
Verifier/Issuer Site
Digital Credentials API
Verifier/Issuer Native App
Credential Manager
VDC
VDC
OS credential management API for browsers
OS version of Digital Credentials API for native apps
OS credential management API for credential managers
OS Platform APIs
Operating System Platform Services
Device


Browser
Verifier/Issuer Site
Digital Credentials API
Verifier/Issuer Native App
Credential Manager
VDC
VDC
OS credential management API for browsers
OS version of Digital Credentials API for native apps
OS credential management API for credential managers
OS Platform APIs
Operating System Platform Services
FIDO CTAP 2.2
OS Platform APIs
Operating System Platform Services
Local Device
Nearby Device

Browser (web platform)	**OS Platform** (app platform)	**Credential Manager** (app/wallet)
<<<<< Permission >>>>>		Holder consent
API surface	Credential selector (presentation)	Holder verification
Basic request validation	Credential manager selector (issuance)	Presentation & issuance protocols (verifier / RP authentication, policy selective disclosure, signing, encryption)
Secure context validation	Cross-device transport	
Interaction with OS platform	Native app requests	Key management

Browser
(web platform)

OS Platform
(app platform)

Credential Manager
(app/wallet)

<<<<< Permission >>>>>

API surface

Basic request validation

Secure context validation

Interaction with OS platform

Credential selector
(presentation)

Credential manager selector
(issuance)

Cross-device transport

Native app requests

Holder consent

Holder verification

Presentation & issuance protocols

(verifier / RP authentication, policy selective disclosure, signing, encryption)

Key management

Browser
(web platform)

OS Platform
(app platform)

Credential Manager
(app/wallet)

<<<<< Permission >>>>>

API surface

Basic request validation

Secure context validation

Interaction with OS platform

Credential selector
(presentation)

Credential manager selector
(issuance)

Cross-device transport

Native app requests

Holder consent

Holder verification

Presentation & issuance protocols

(verifier / RP authentication, policy selective disclosure, signing, encryption)

Key management

Browser
(web platform)

OS Platform
(app platform)

Credential Manager
(app/wallet)

<<<<< Permission >>>>>

API surface

Basic request validation

Secure context validation

Interaction with OS platform

Credential selector
(presentation)

Credential manager selector
(issuance)

Cross-device transport

Native app requests

Holder consent

Holder verification

Presentation & issuance protocols

(verifier / RP authentication, policy selective disclosure, signing, encryption)

Key management

European Commission | EU Digital Identity Wallet

Browser (web platform)	**OS Platform** (app platform)	**Credential Manager** (app/wallet)
<<<<< Permission >>>>>		Holder consent
API surface	Credential selector (presentation)	Holder verification
Basic request validation	Credential manager selector (issuance)	Presentation & issuance protocols
Secure context validation	Cross-device transport	(verifier / RP authentication, policy selective disclosure, signing, encryption)
Interaction with OS platform	Native app requests	Key management

<<<<< Permission >>>>>

Browser
(web platform)

API surface

Basic request validation

Secure context validation

Interaction with OS platform

OS Platform
(app platform)

Credential selector
(presentation)

Credential manager selector
(issuance)

Cross-device transport

Native app requests

Credential Manager
(app/wallet)

Holder consent

Holder verification

Presentation & issuance protocols

(verifier / RP authentication, policy selective disclosure, signing, encryption)

Key management

RP Perspectives

Andreea Stefan

Product Area Lead
@ ING Global Platform

(Authentication, ID&V, Approval & Consent)

ING Factory

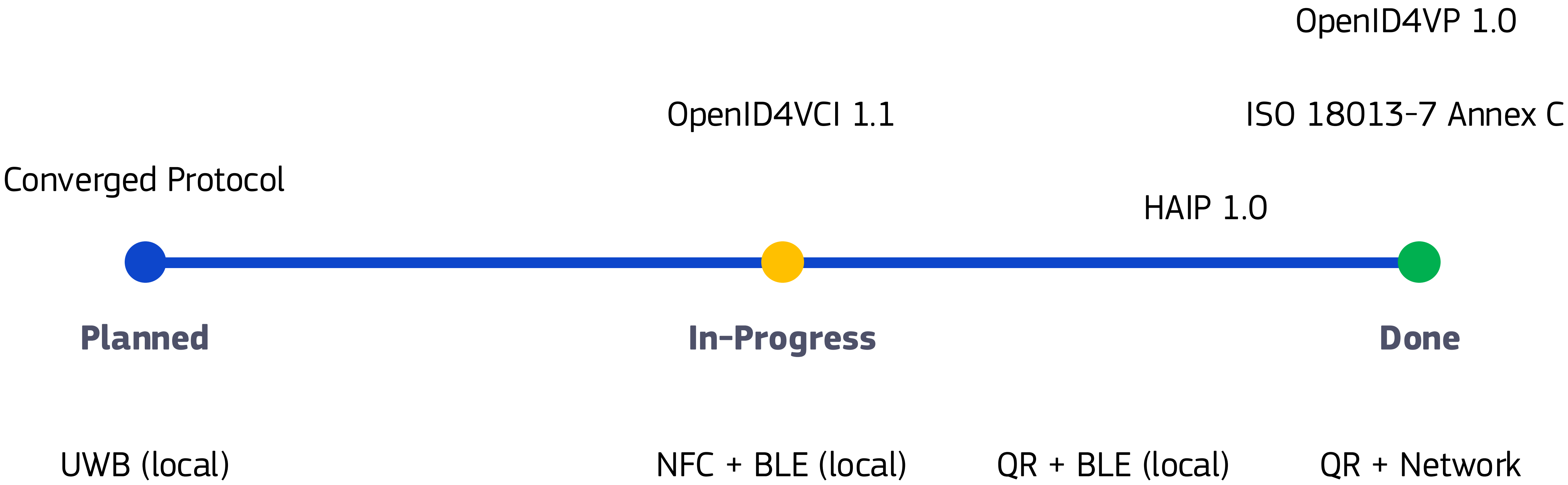
ideas worth building

Let’s stay connected!

I’d love to connect and continue the conversation.

Status & Timelines

EXCHANGE PROTOCOLS



OpenID4VP 1.0

OpenID4VCI 1.1

ISO 18013-7 Annex C

Converged Protocol

HAIP 1.0

Planned

In-Progress

Done

UWB (local)

NFC + BLE (local)

QR + BLE (local)

QR + Network

CROSS-DEVICE PROTOCOL

Current Work Items

STATUS & TIMELINES

DIGITAL CREDENTIALS API

- Finalizing issuance (*navigator.credentials.create*)

ECOSYSTEM

- Additional transports for cross-device presentation and issuance
- Protocol convergence
- UX research and developer resources

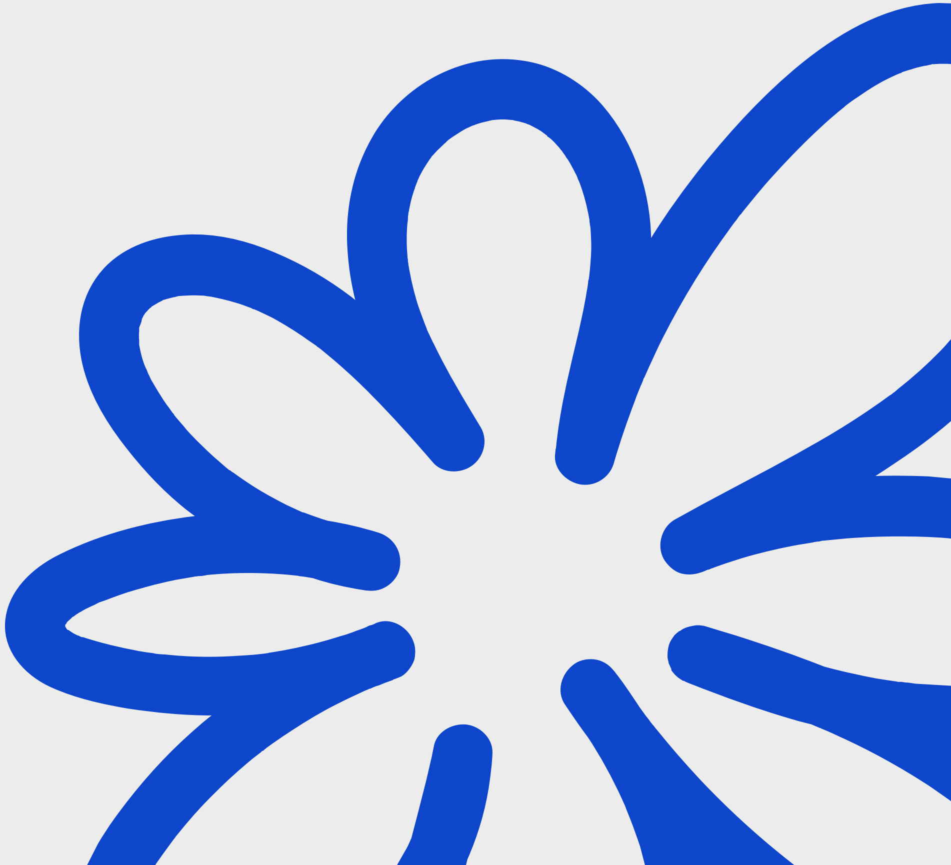
More Details

STATUS & TIMELINES

digitalcredentials.dev > Ecosystem Support

Time for questions!

Thank You!



European Commission

EU Digital Identity Wallet