Real World Identity on the Web... continued

Tim Cappalli | Heather Flanagan

TPAC 2024
Anaheim CA, USA
hybrid meeting
23–27 SEPTEMBER 2024

Agenda

- Background, Concepts, and Scope (15m)
- Demo: Digital Credentials API + Google Wallet (10m)
- PING / privacy related discussions (Nick Doty) (10m)
- Unlinkability and Google's ZKP solution for predicates (10m)
- Gaps and Next Steps (15m)

Background, Concepts & Scope

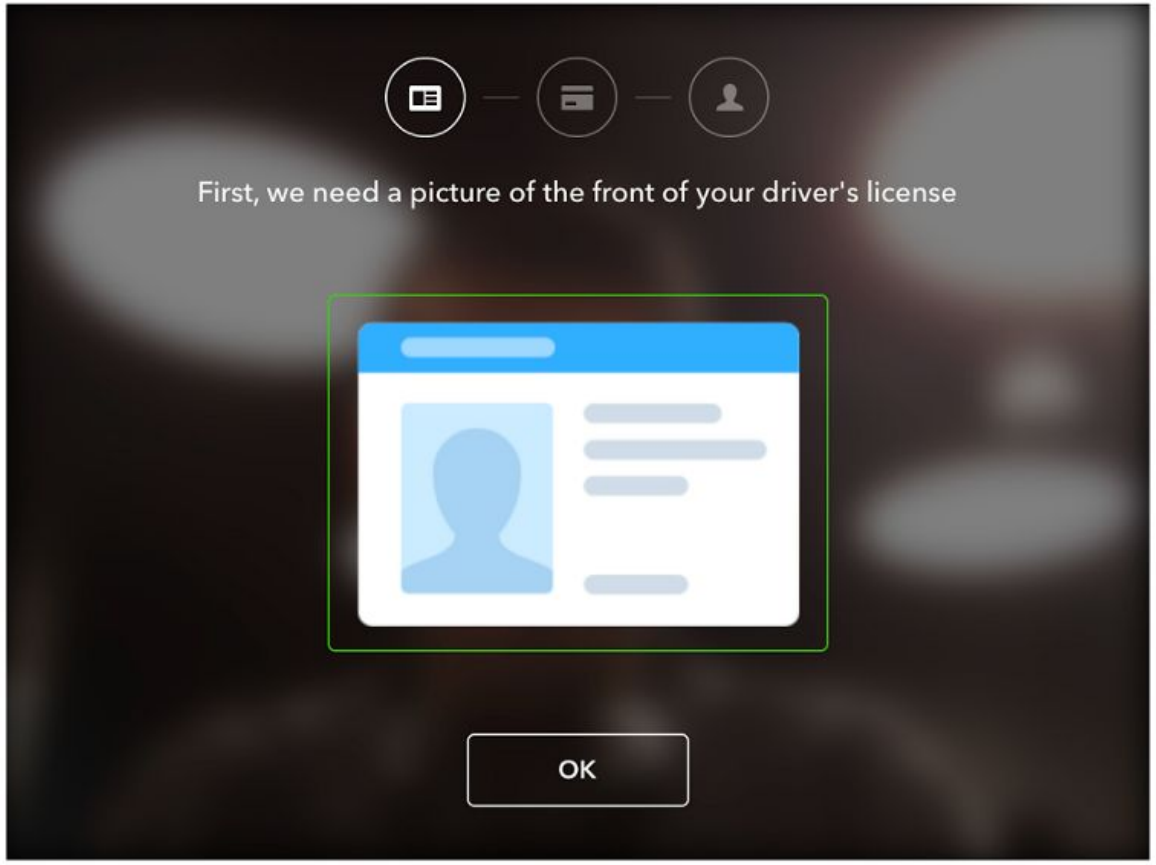
The Problem, Gen 1

Document Verification

Back to Limits

Example

- **Turn up your brightness** and avoid glare
- **First name** and **last name** clearly visible
- **Date of birth** clearly visible
- **ID number** clearly visible
- **Fully in frame**, not cut off on any side



The Problem, Gen 2

digital credential presentation on the web currently relies on primitives such as ***custom schemes*** *and* ***QR codes*** *which have* ***poor security properties*** *and an even* ***worse user experience***

What is a custom URL scheme?

A custom identifier that an app can register with an operating system with the goal of being invoked from other contexts, such as other apps or from the web.

In many cases, these identifiers are not globally unique, and may be shared.

CUSTOM SCHEMES IN THE WILD

mdoc://

openid4vp://

eudi-wallet://

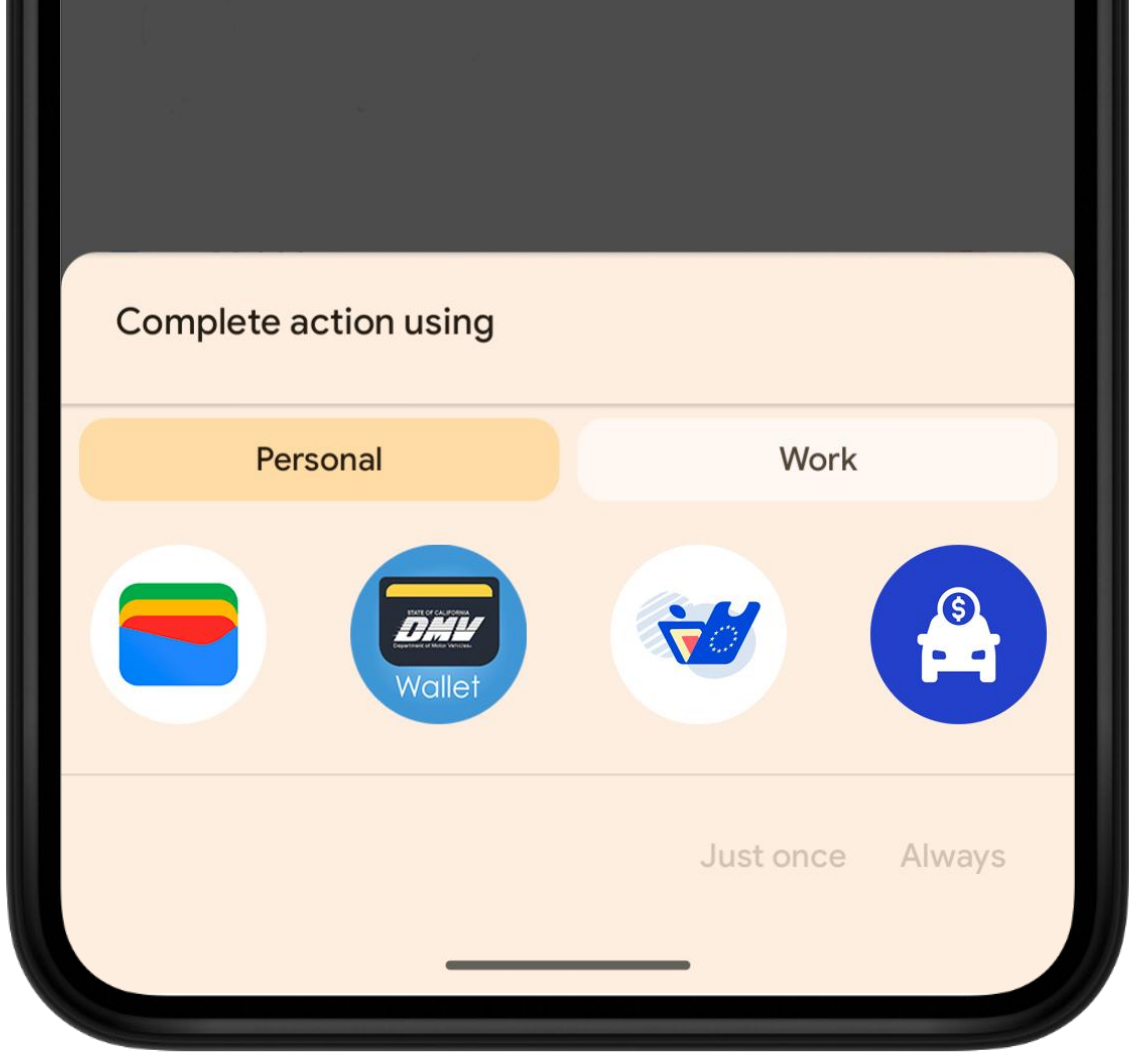
eudi-openid4vp://

mdoc-openid4vp://

openid-credential-offer://

Issues w/ custom schemes

- invocation from insecure contexts
- on-device phishing via app selection
- no requestor origin / identity
- not standardized & not guaranteed
- context switch during app launch
- no graceful fallback for errors



poor UX for credential selection

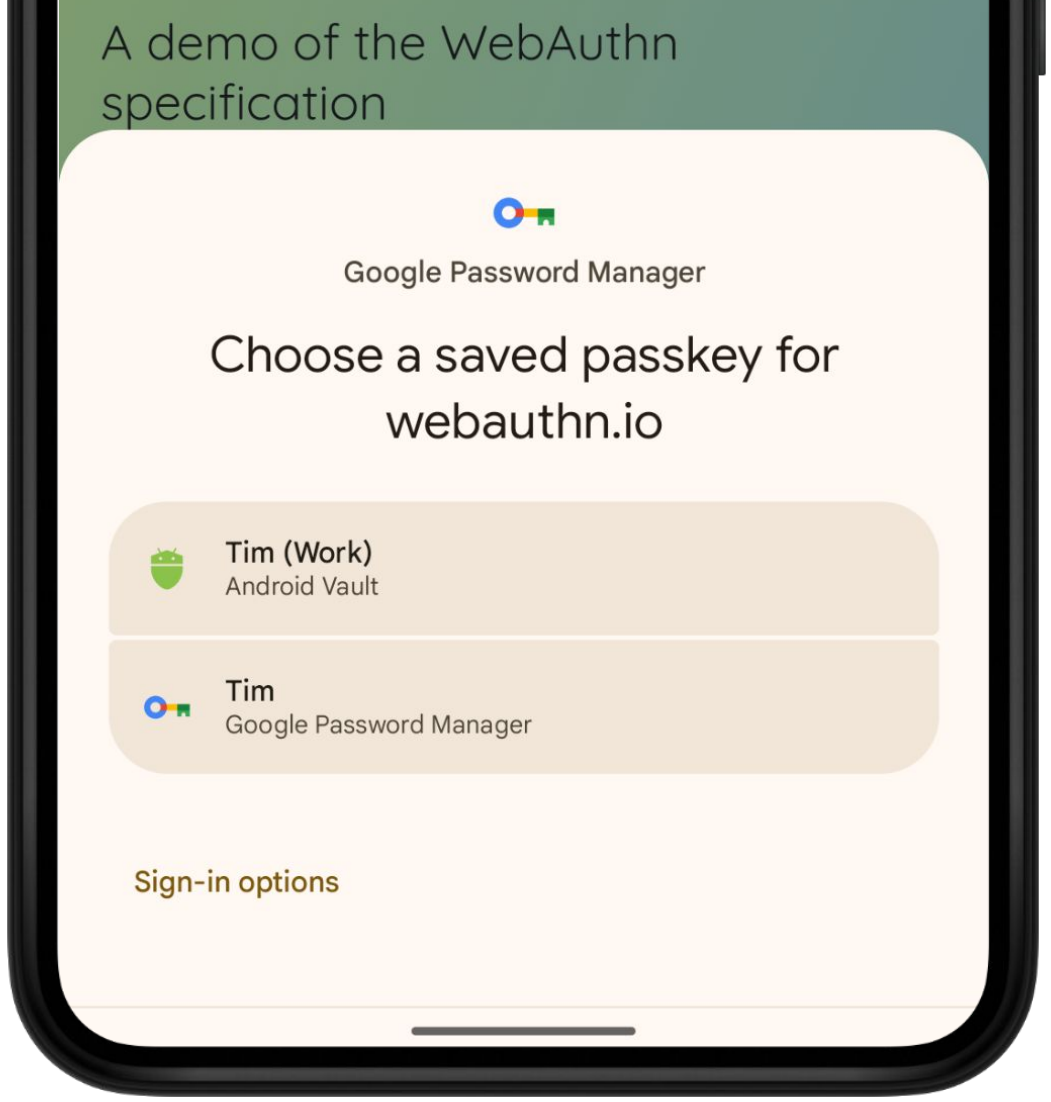
(*users don't understand wallet selection*)

Learnings from passkeys

users think about **accounts** and **credentials**, not **authenticators**

caller context is key

cross-device authentication needs to be **secure**, **easy**, and **resistant to phishing**



How We Got Here

FIDO Wallet Task Force

Internet Identity Workshop

WICG Work Item

OpenID Digital Credentials Protocols WG Collab

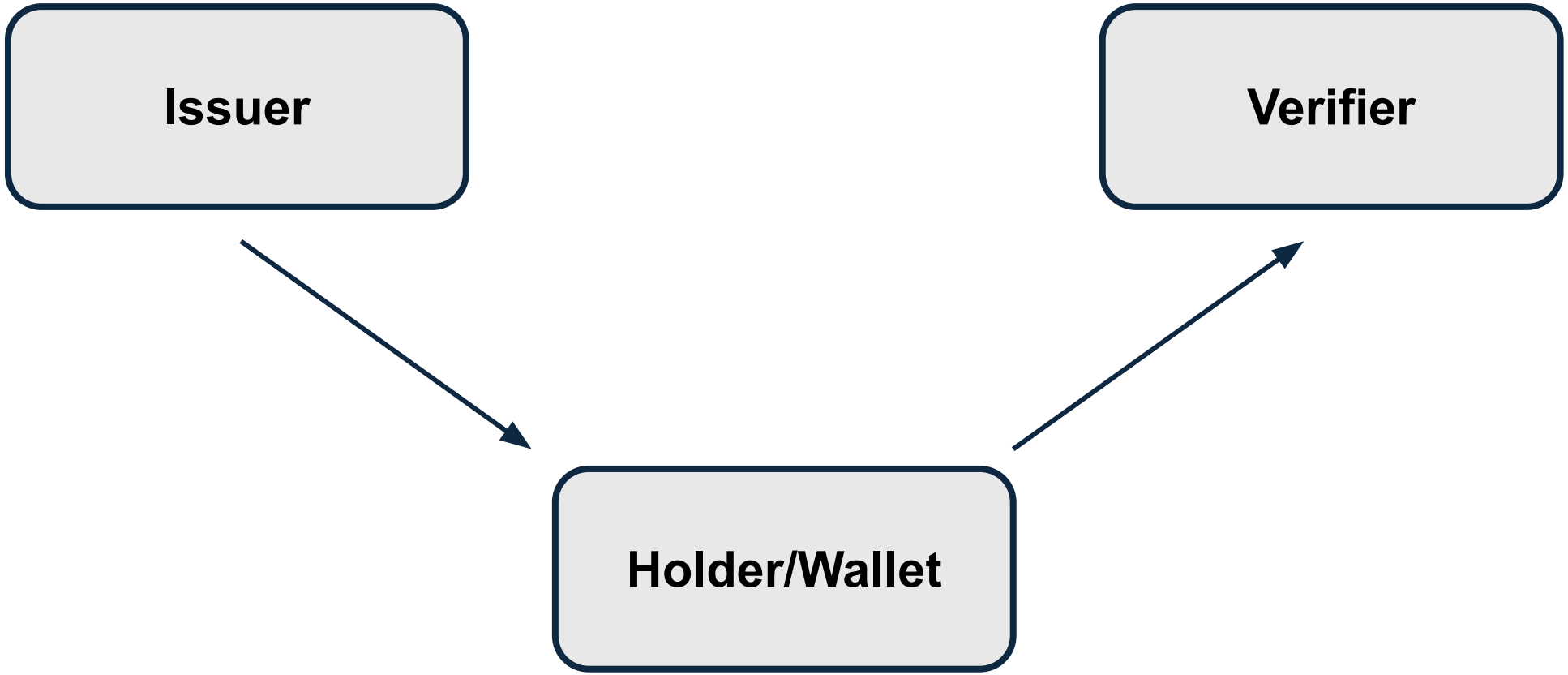
W3C Federated Identity WG

2021

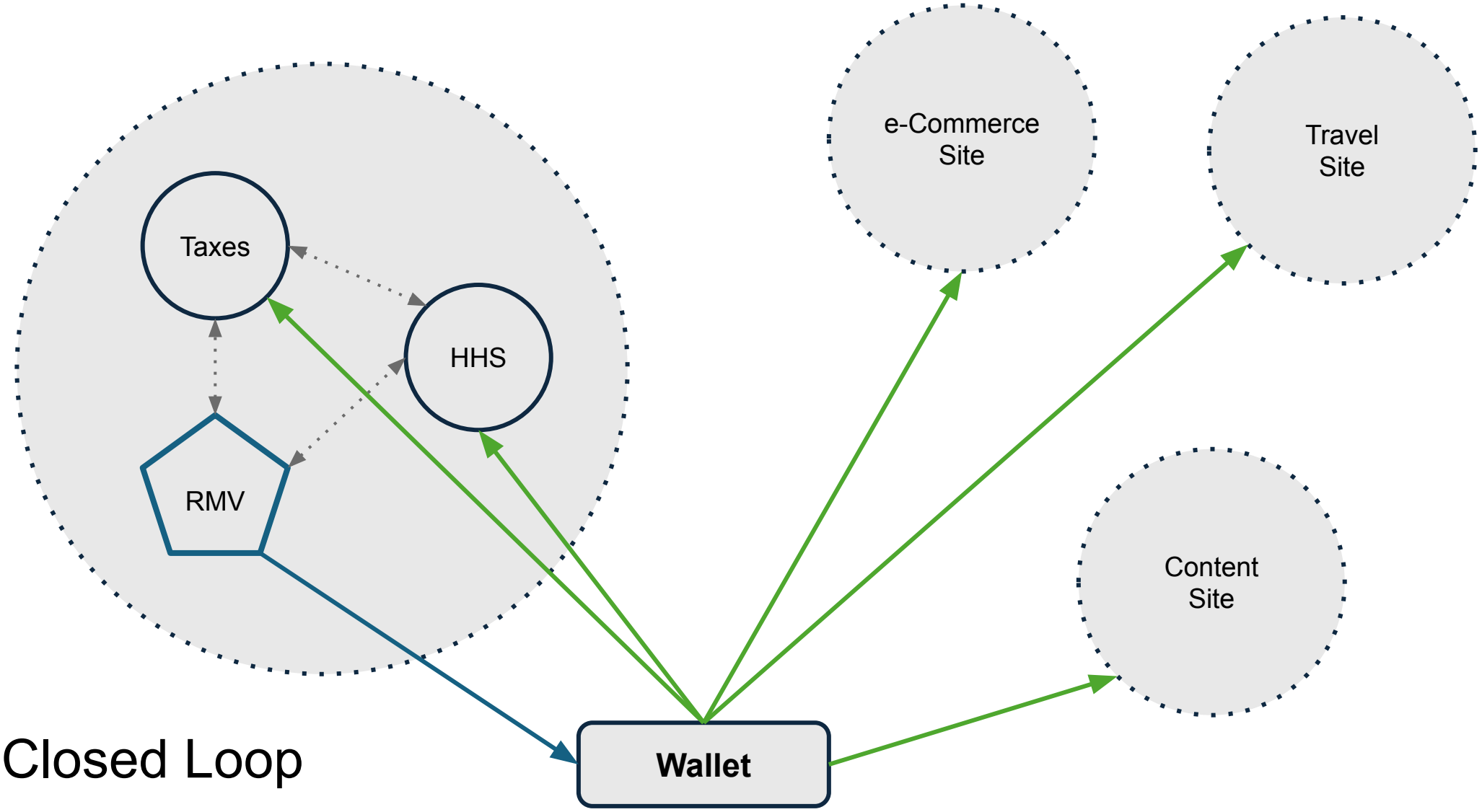
2023

Future

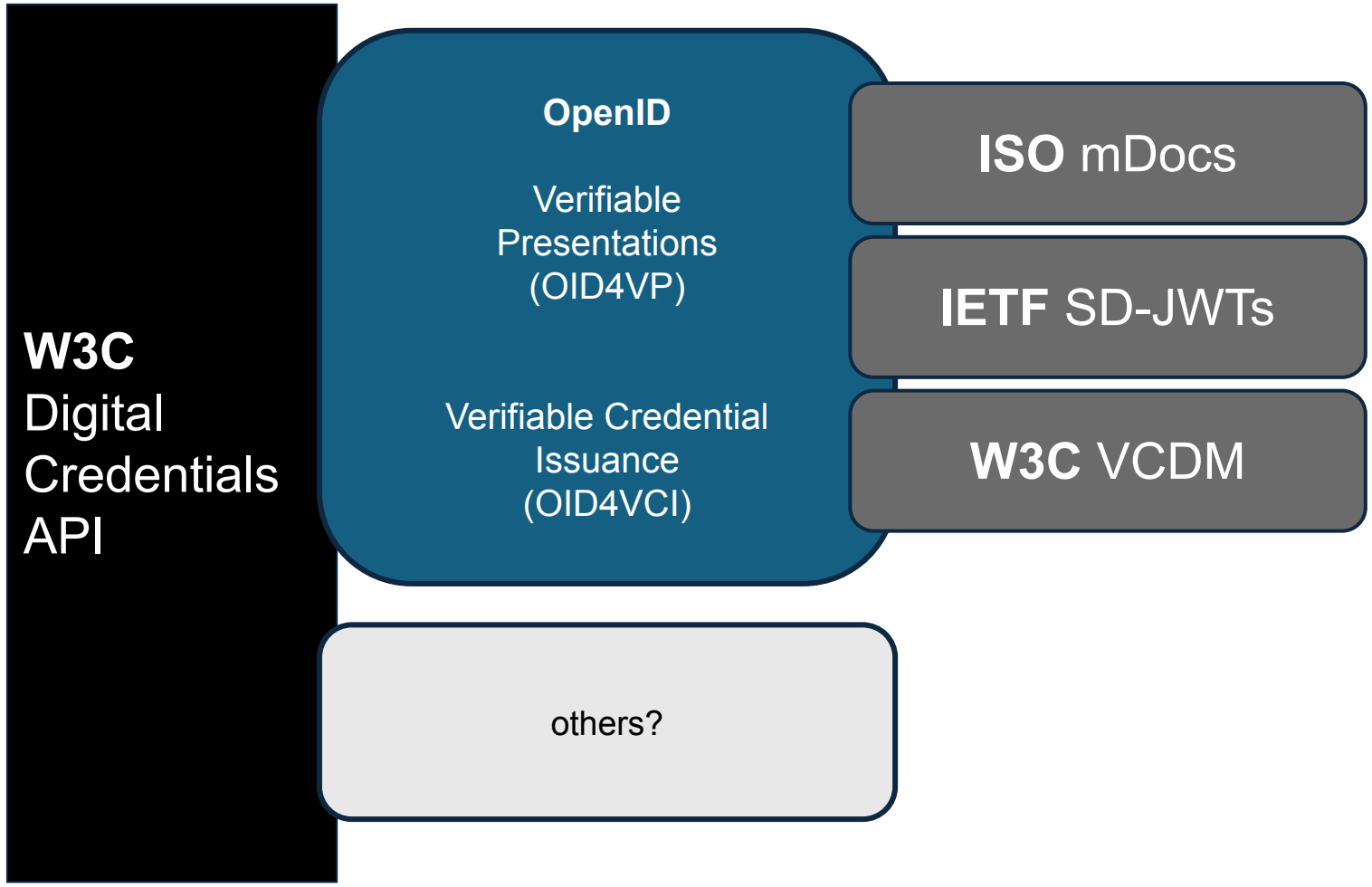
Concepts

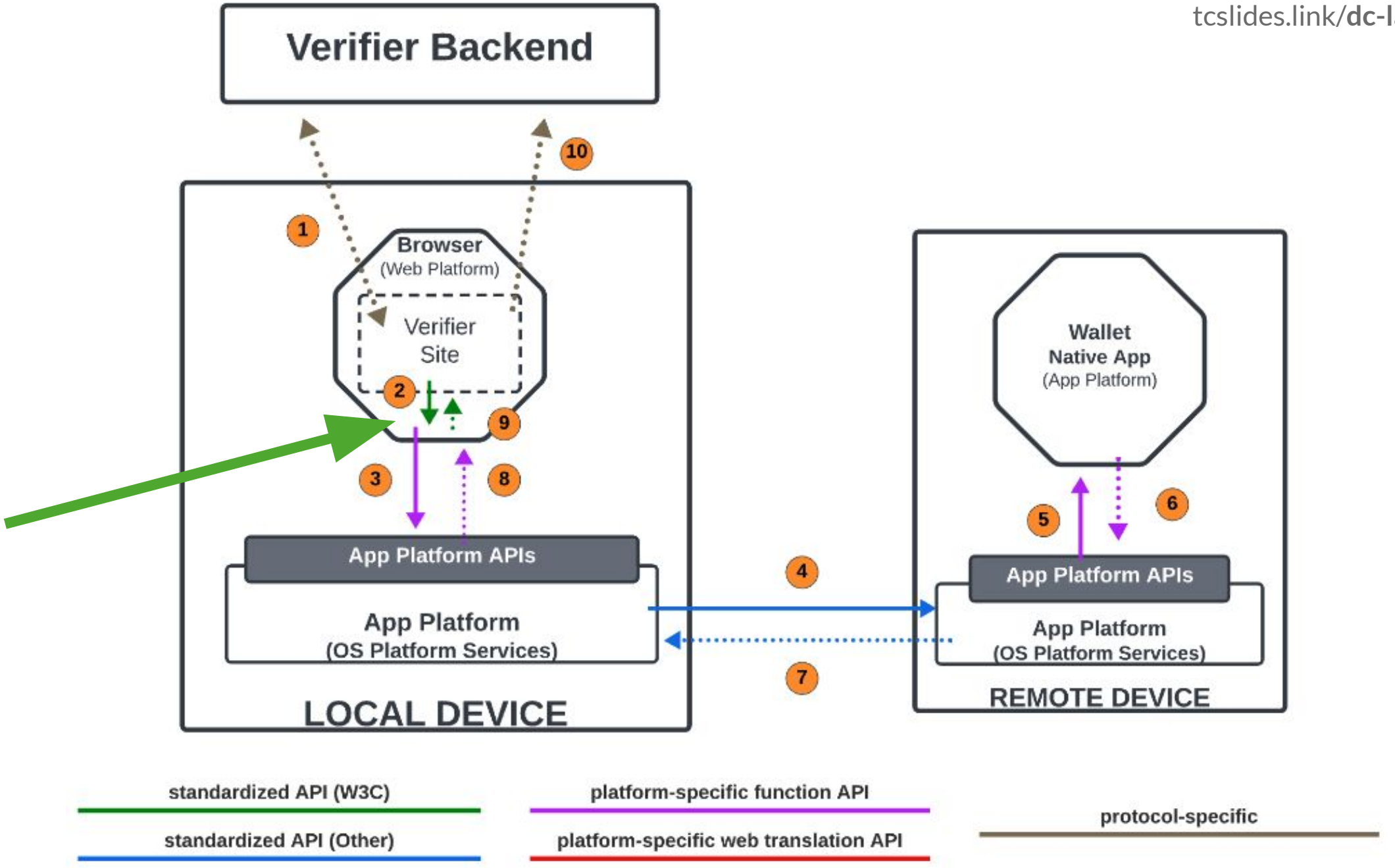


Concepts


Open Loop
e-Commerce Site
Travel Site
Taxes
HHS
RMV
Content Site
Closed Loop
Wallet

Layers

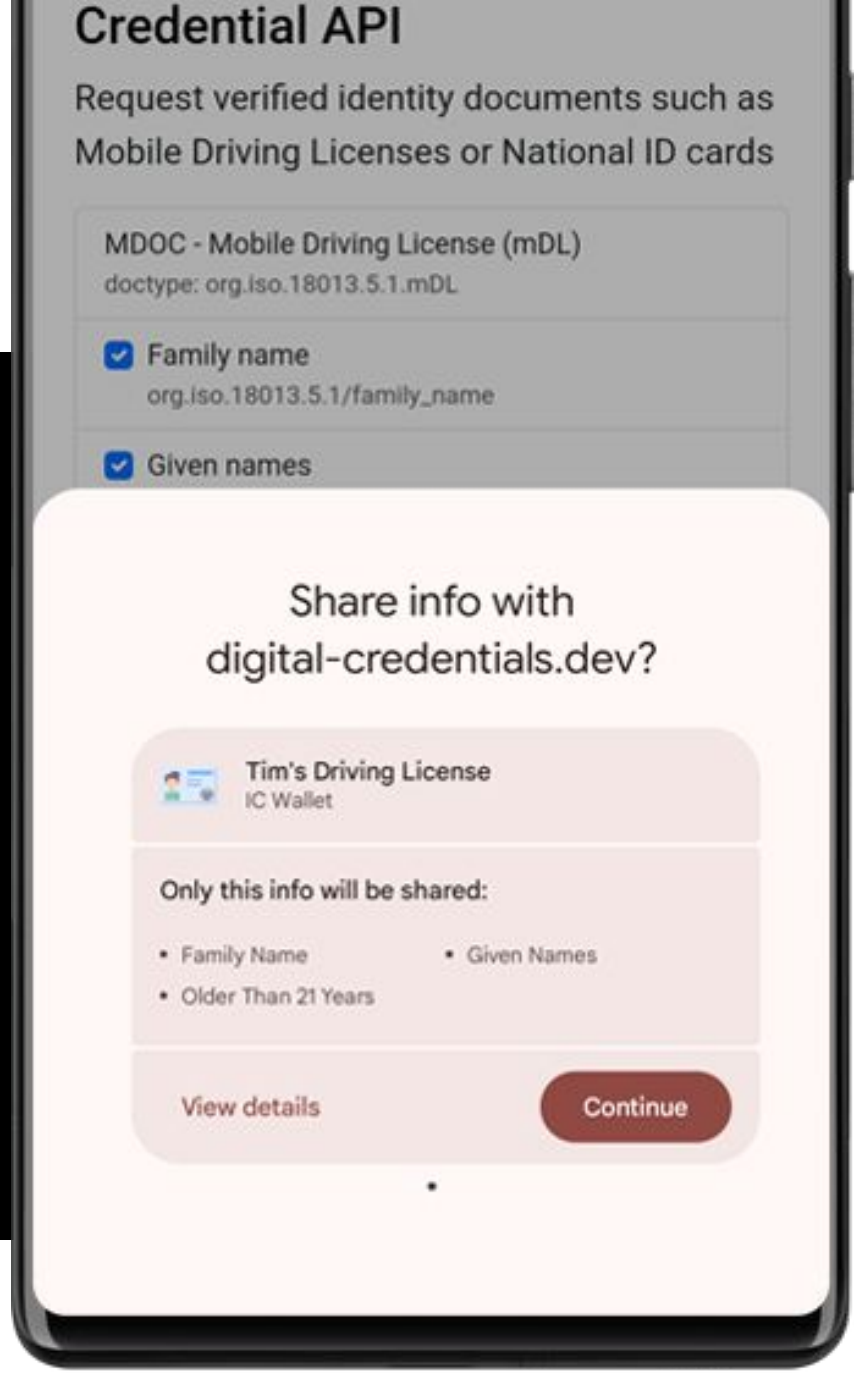

W3C
Digital
Credentials
API
OpenID
Verifiable
Presentations
(OID4VP)
Verifiable Credential
Issuance
(OID4VCI)
others?
ISO mDocs
IETF SD-JWTs
W3C VCDM
protocols
credential
formats


Verifier Backend
10
1
Browser
(Web Platform)
Verifier
Site
2
9
3
8
App Platform APIs
App Platform
(OS Platform Services)
LOCAL DEVICE
4
7
Wallet
Native App
(App Platform)
5
6
App Platform APIs
App Platform
(OS Platform Services)
REMOTE DEVICE
standardized API (W3C)
standardized API (Other)
platform-specific function API
platform-specific web translation API
protocol-specific

Demo

The API

```
let digiCred = await
  navigator.credentials.get({
        signal: controller.signal,
        digital: {
          requests: [{
            protocol: "openid4vp",
            data: "{request json}"
          }]
        }
    });
```



PING / Privacy Discussion

Unlinkability and Google’s ZKP solution for predicates

ZKP Design Goals

1. work with existing hardware and software in the wild (certified, vetted implementations)
   a. ECDSA as signature scheme for issuer
   b. ECDSA & passkey on user devices
   c. Software that does not deal with cryptographic keys can change

2. privacy for users
   a. selective disclose of attributes
   b. issuer-verifier unlinkability
   c. verifier-verifier unlinkability

3. same security as “traditional credentials”
   a. unforgeable:
      i. users cannot produce attributes that were not issued to them
      ii. no mix and match of attributes
   b. assumes security of hardware (user and issuer side)

Gaps and Next Steps