A Perspective on Digital Identity

Global Platform Summit
March 2024

David Zeuthen (zeuthen@google.com)

Important note!

Everything in this presentation reflects our current ideas and thinking.

The broad strokes are *probably* accurate. **Details will certainly change. Don't depend on anything until it's released.**

Agenda

- About me
- OWF Identity Credential project
- Google Wallet
- Android and Security

About Me

- **David Zeuthen**

- **Software Engineer at Google in the Android Security and Privacy Team**
  - Involved in hardware-backed security and OS security (TEEs, SEs, bootloaders, etc)
  - Working with both 1P and 3P application providers and hardware OEMs

- **Been involved with Digital Identity since 2018**
  - Member ISO/IEC JTC1 SC17 WG4 and WG10 (23220 series, 18013-5/7)
  - Member W3C WICG for Digital Identities

- **OpenWallet Foundation TAC Member**

- **Maintainer of OWF Identity Credential project**

- **Passionate about the intersection of UX and security/privacy**

OWF Identity Credential

OWF Identity Credential

- **What is it?**
  - Libraries and applications for Real-World Identity
  - Initial focus was Android and mDL according to ISO/IEC 18013-5:2021
  - Current focus includes iOS, server-side, and multiple credential formats

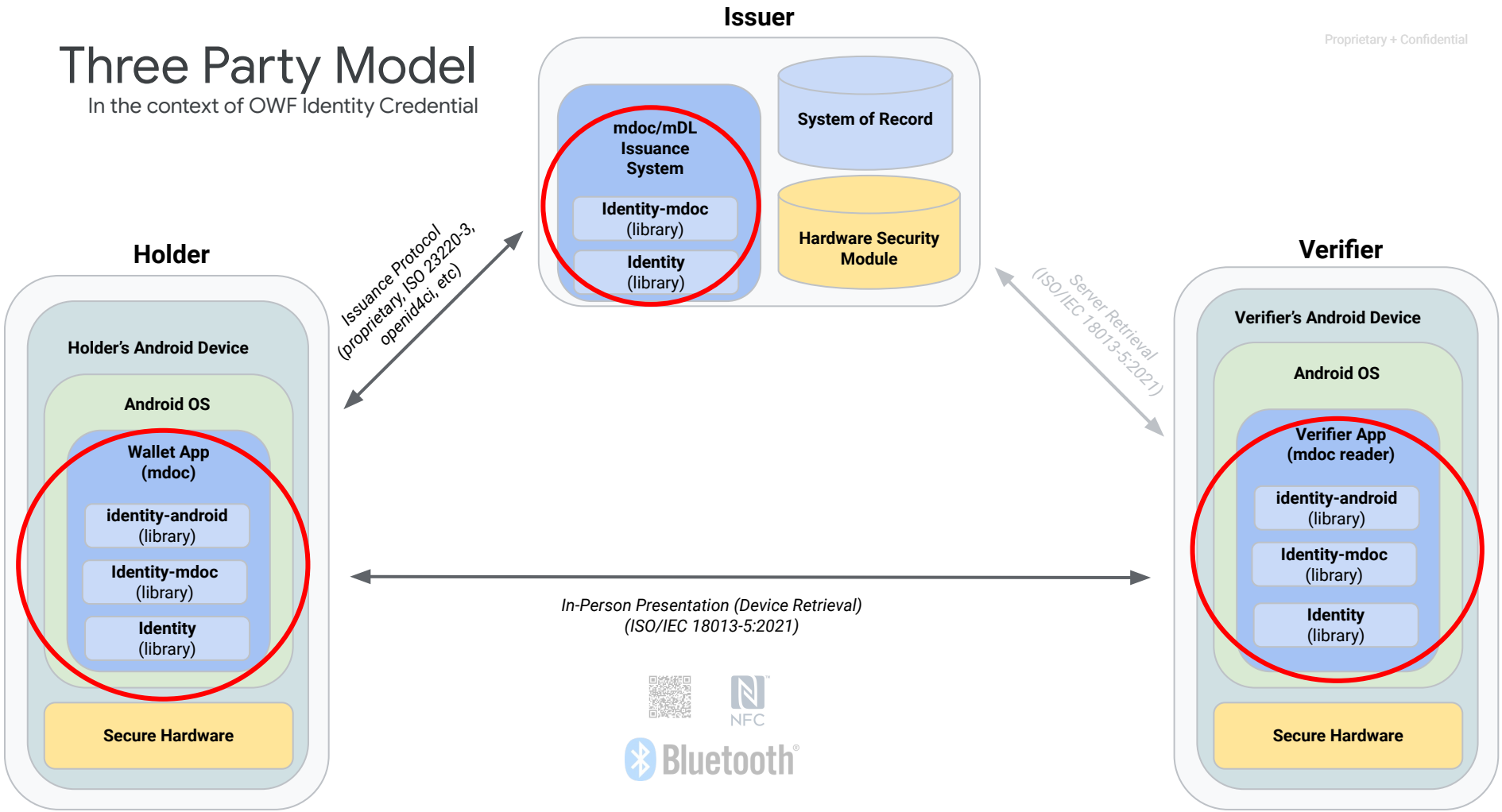
- **Hosted at https://github.com/openwallet-foundation-labs/identity-credential**
  - Available since 2019 under Apache2 license
  - An OpenWallet Foundation project since fall 2023

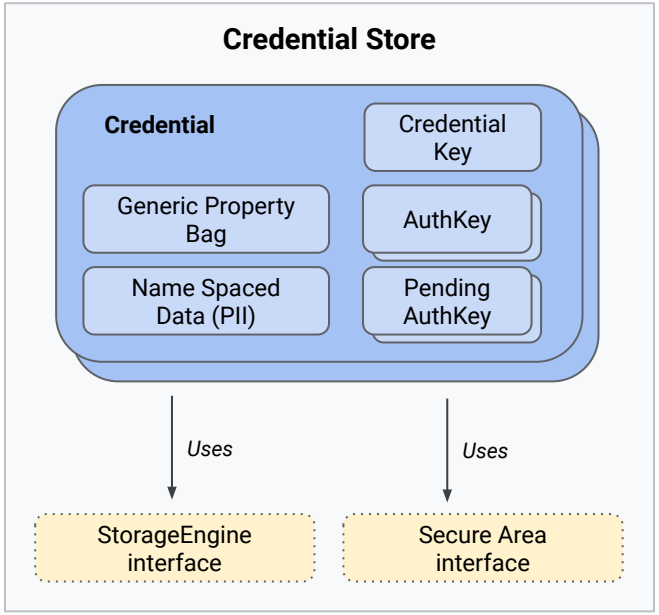
- **Implements issuance/provisioning, storage, presentment, and verification of mDL/mdocs**
  - Implements ISO/IEC 18013-5:2021 for presentment (mdoc and mdoc reader)
    - Currently used in production apps on Android
  - Issuance and user proofing
    - Our current focus
  - Uses hardware-backed keystore and remote attestation

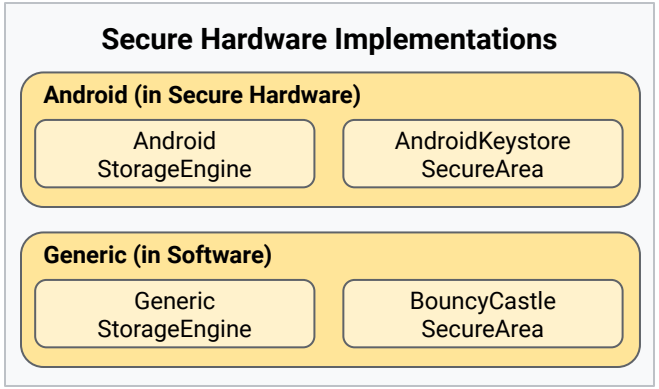
- **Production-quality library stack**
  - Been to most ISO SC17 WG10 organized mDL interoperability events, can pass UL certifications
  - Used in several wallet projects, including Google Wallet and EUDI Wallet Reference Code
  - Strong focus on testability

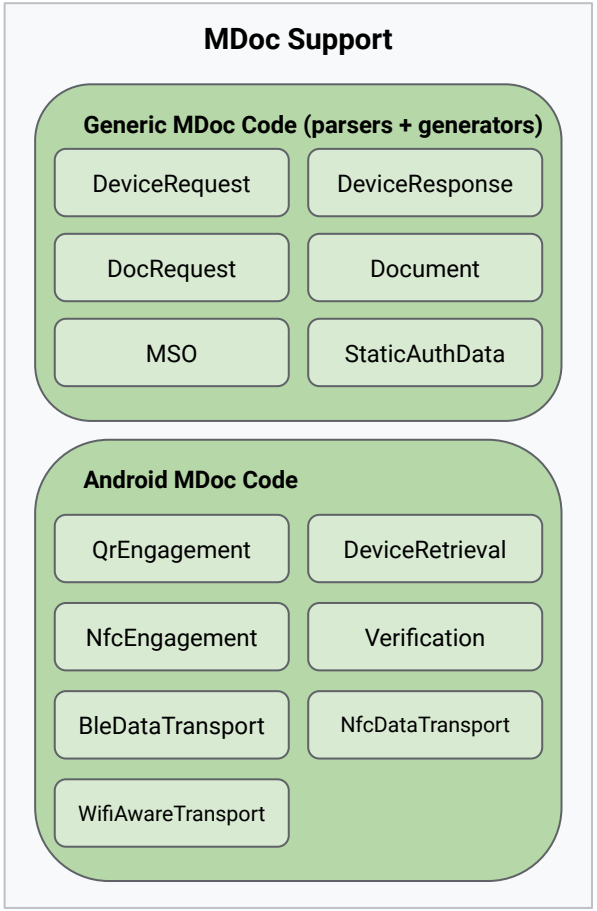
Three Party Model

In the context of OWF Identity Credential





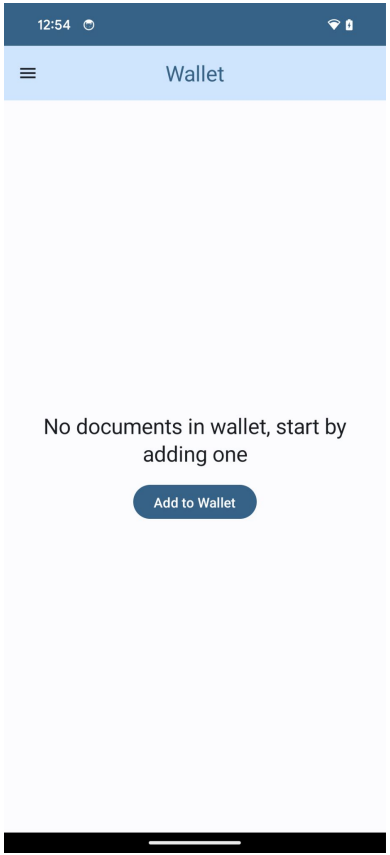


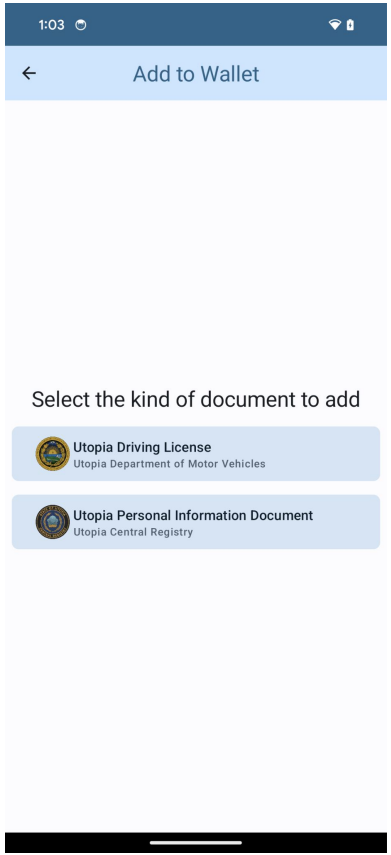


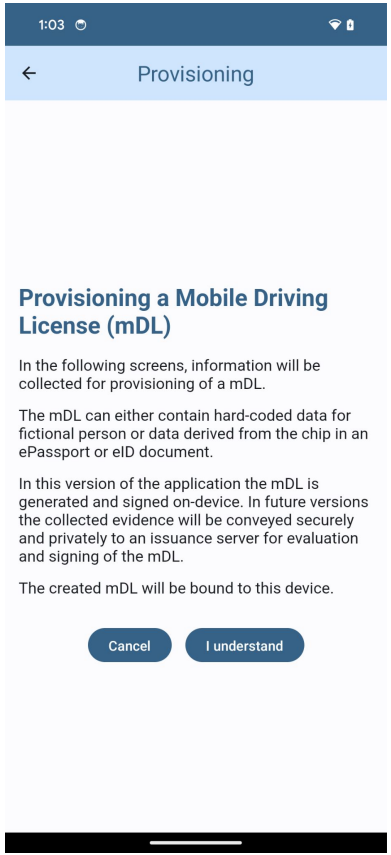
- **No explicit Android dependencies**: designed to also be used server side e.g. for issuance and verification. Also useful for unit testing.
- **No explicit MDoc dependency:** library can just as easily be used for W3C VCs as for MDoc. Maps well to e.g. SD-JWT
- **Secure Area and storage abstraction:** library includes Android Keystore implementation (for HW-backed keys) but application can easily include its own implementation for communicating with proprietary Cloud or Secure Element secure areas
- **Batteries included:** library includes production-quality Wallet (Holder) and Reader (Verifier) apps

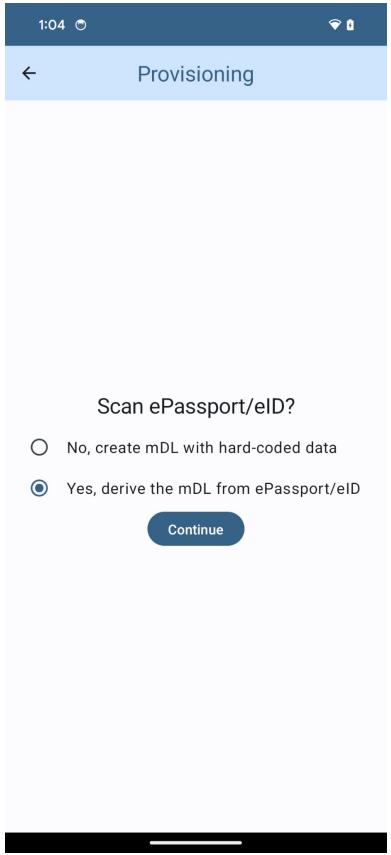
Demo

Wallet - Provision Credential

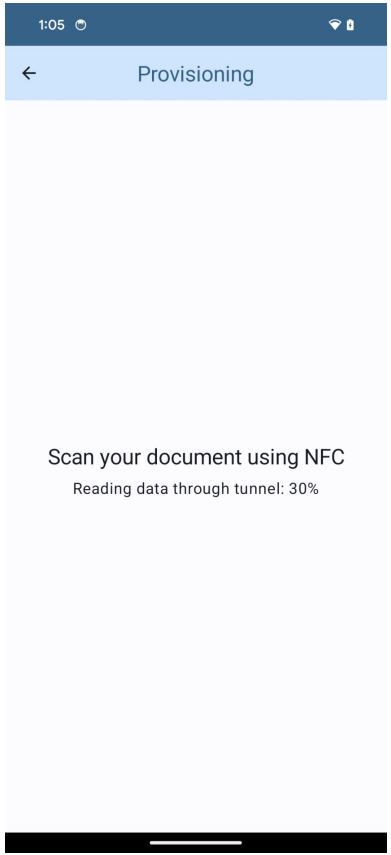


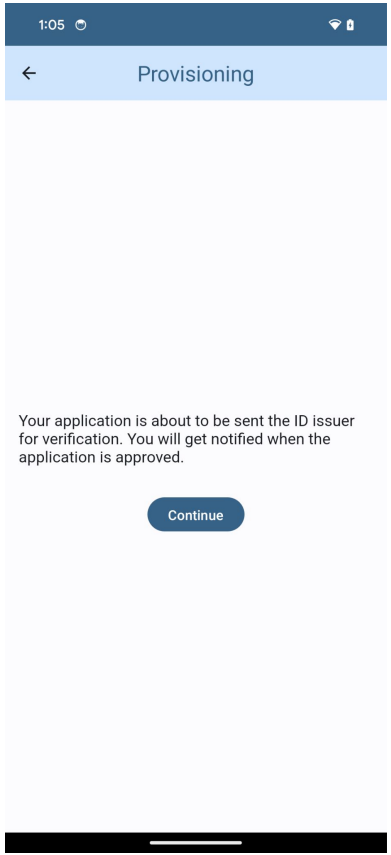


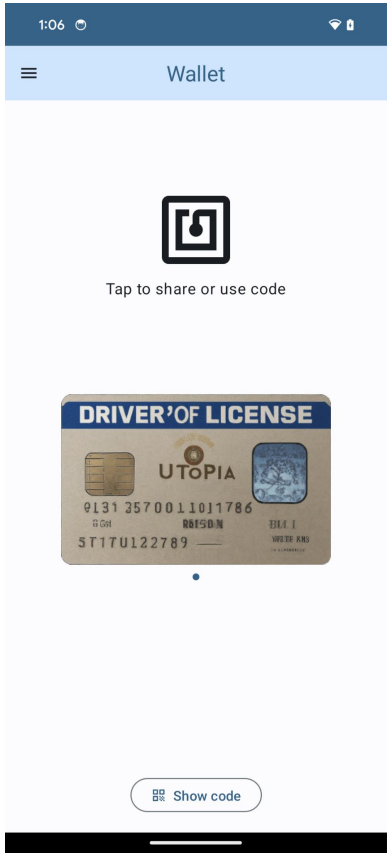




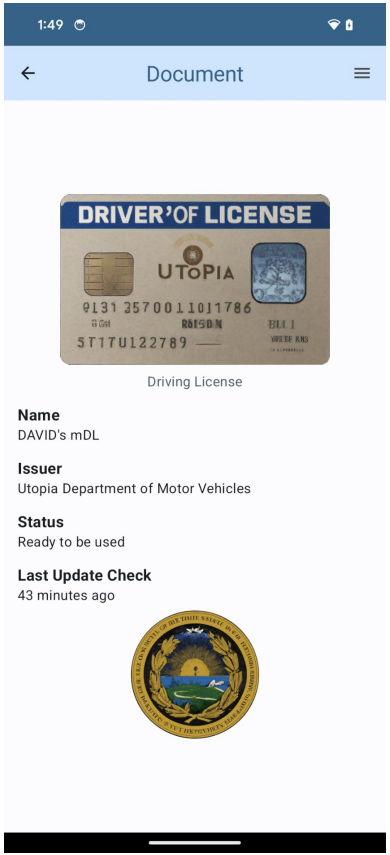
Wallet - Provision Credential

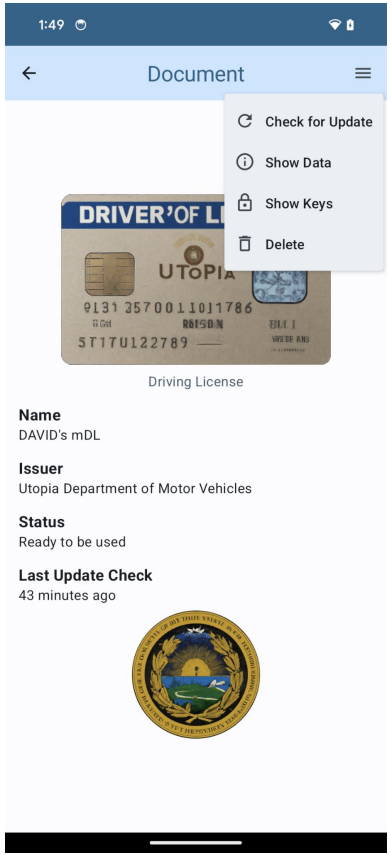


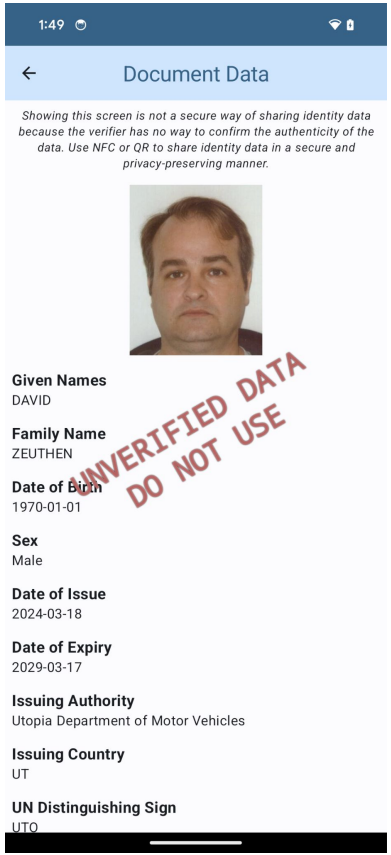


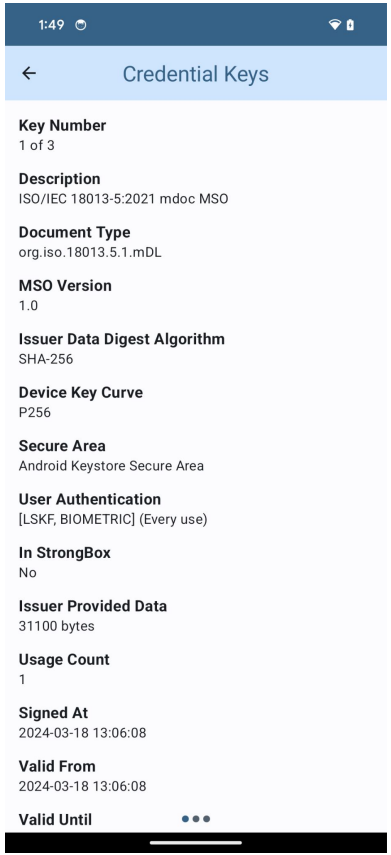


Wallet - Credential Information

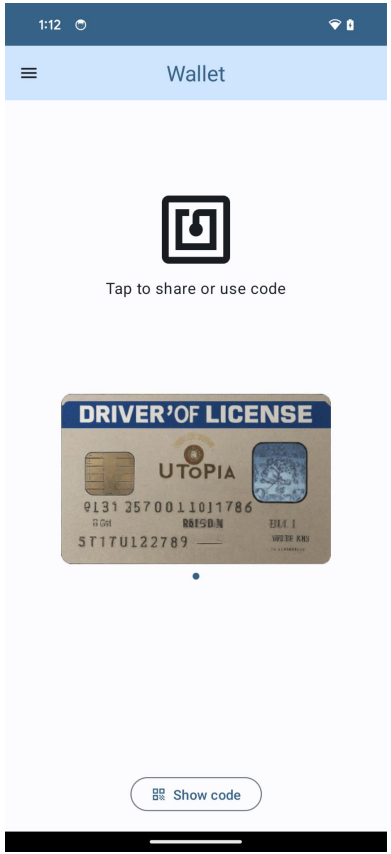


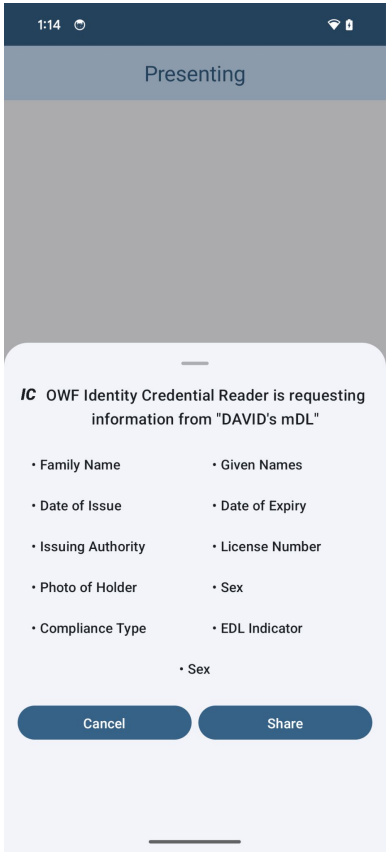






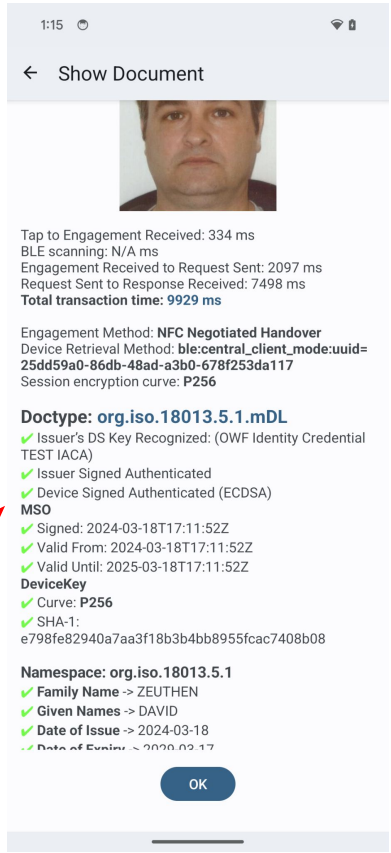
Wallet - Proximity Sharing (ISO/IEC 18013-5:2021)





Holder's Device

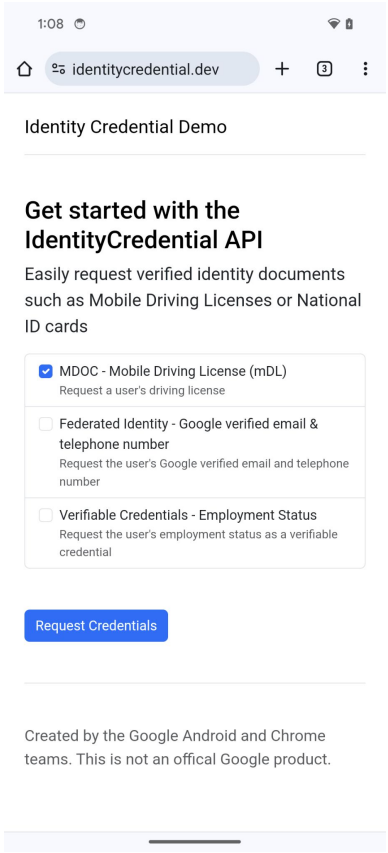
Checkmarks indicates the data was cryptographically verified and thus trustworthy

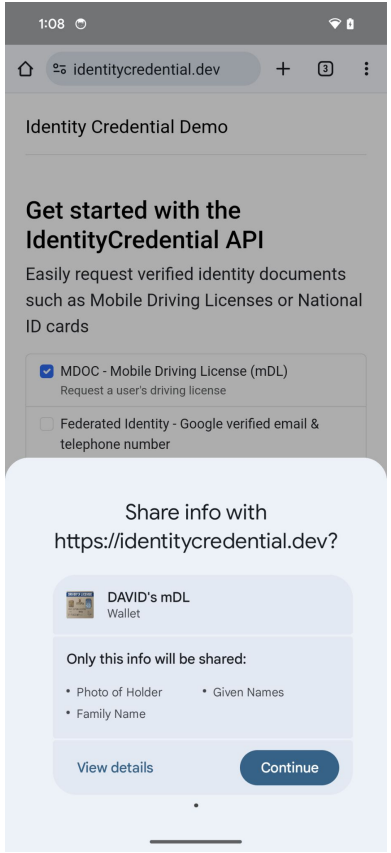


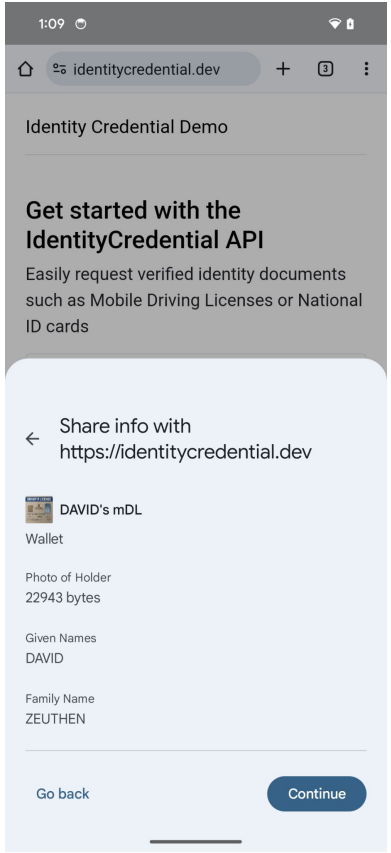
Verifier's Device

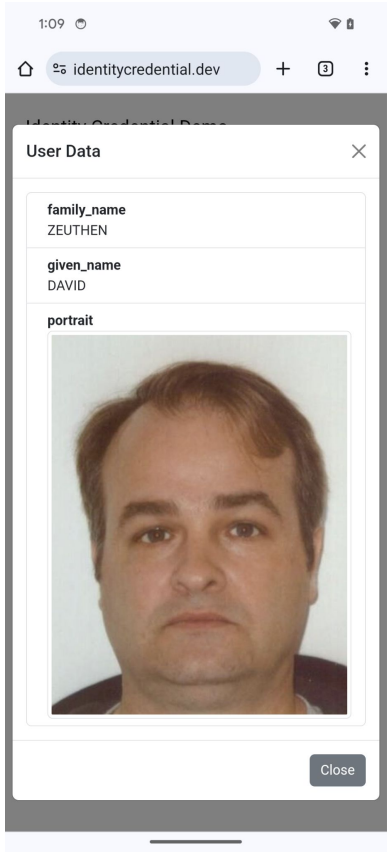
Wallet - Proximity Sharing (ISO/IEC 18013-5:2021)

Wallet - Share to Website (W3C WICG Digital Identities)









Google

OWF Identity Credential roadmap

- **Integration with https://github.com/WICG/digital-identities**
  - A way to present identity credentials through the web browser
    - Including x-device and x-platform
  - Actively working with other industry partners and SDOs in the W3C

- **Working with Android and Chrome teams to add native rich APIs for Real-World Identity**

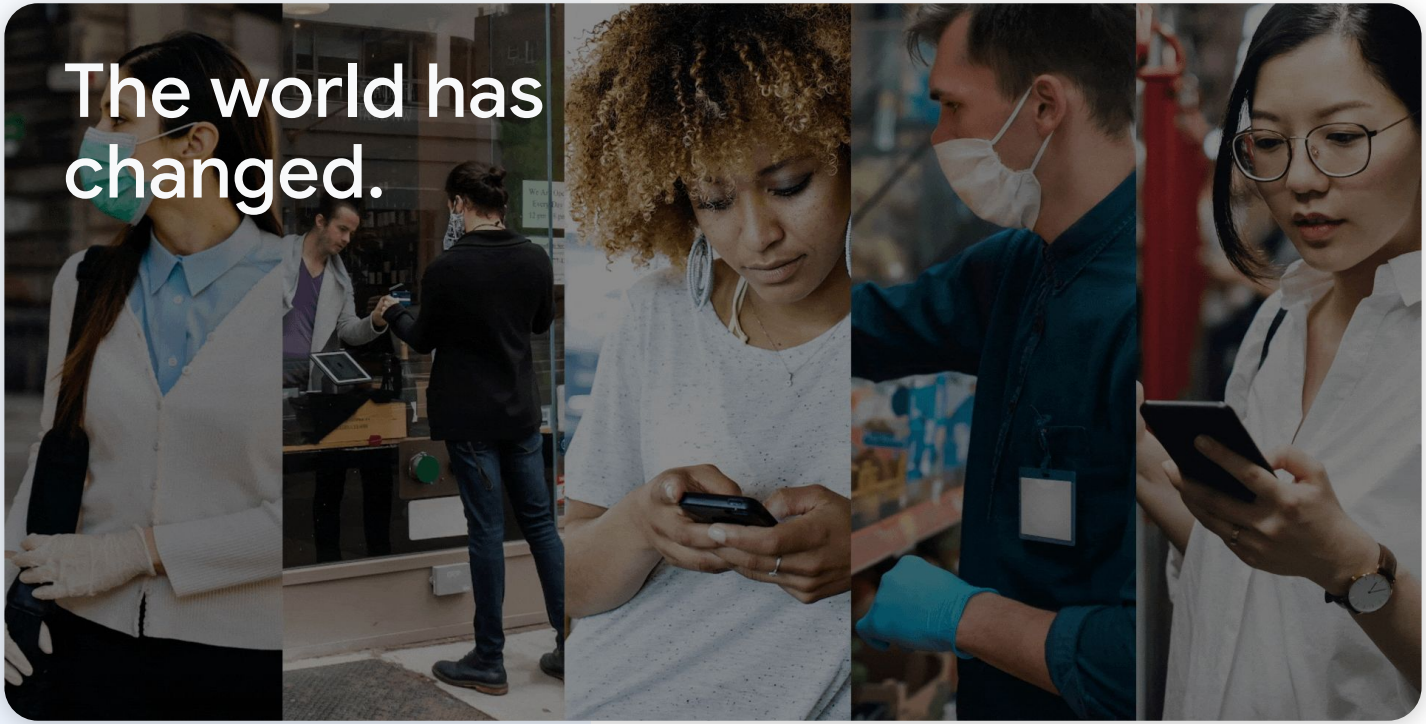
- **Low-power / direct-access use-case**
  - We're writing an open-source Java Card to facilitate mDL/mdoc presentment when the phone is out of battery (but has enough battery to power the NFC chip)

- **Focus areas:**
  - W3C Browser API
  - Issuance and user proofing (including Wallet Server)
  - Making wallet/reader applications production quality
  - iOS support (via Kotlin Multiplatform and Compose Multiplatform)
  - ZKP-based presentation protocols

Credential Formats

- Our libraries and applications are designed to support any credential format
- We have a lot of experience with **mdoc/mDL** from **ISO/IEC 18013-5:2021** and we like it a lot
  - Uses proven cryptography implemented in Secure Hardware on essentially any phone
    - Elliptic Curve Cryptography using ECDSA, ECDH, AES-GCM, etc
  - Excellent security and privacy features for the holder
    - Selective Disclosure
    - Anti-tracking (via one-time-use MSOs)
    - Anti-cloning (via keeping DeviceKey in Secure Hardware)
  - Excellent interoperability profile
  - Broad industry support (wallets, readers, issuance systems, open-source code)
  - Extensible to other document formats than **mDL**

Google Wallet


The world has changed.

The wallet ecosystem is evolving rapidly.

4 billion people are expected to use digital wallets by 2024[1]. Up from 2.3B in 2019

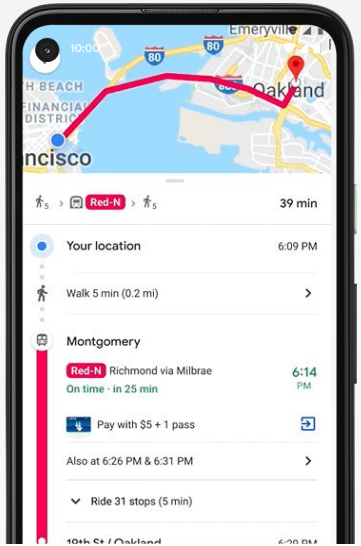
Meet Google Wallet.

It stores your everyday essentials

- Payments
- Identification
- Transit
- Boarding Passes
- Hotel Keys
- Car Keys
- Loyalty
- Health
- Event Tickets

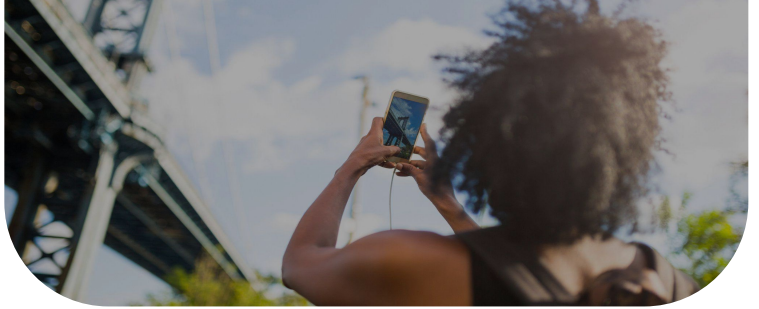
Built for the best experience across Google surfaces

Mock is an illustrative design concept and not final



A vision of the (near) future

Imagine you're heading for weekend trip to explore a new city



Walk to
your coffee shop and use your phone to pay

Take transit
to the airport. Pay with your phone and see your card balance in Google Maps

Go through
security showing your digital driver's license

Find your gate
using your mobile boarding pass

Start your rental
car using your phone

Check in
and open your hotel room with your phone as the key

Tap to pay
for toothpaste at the drugstore, loyalty card is applied automatically

Enter a concert
that evening showing your vaccine card and ticket on your phone

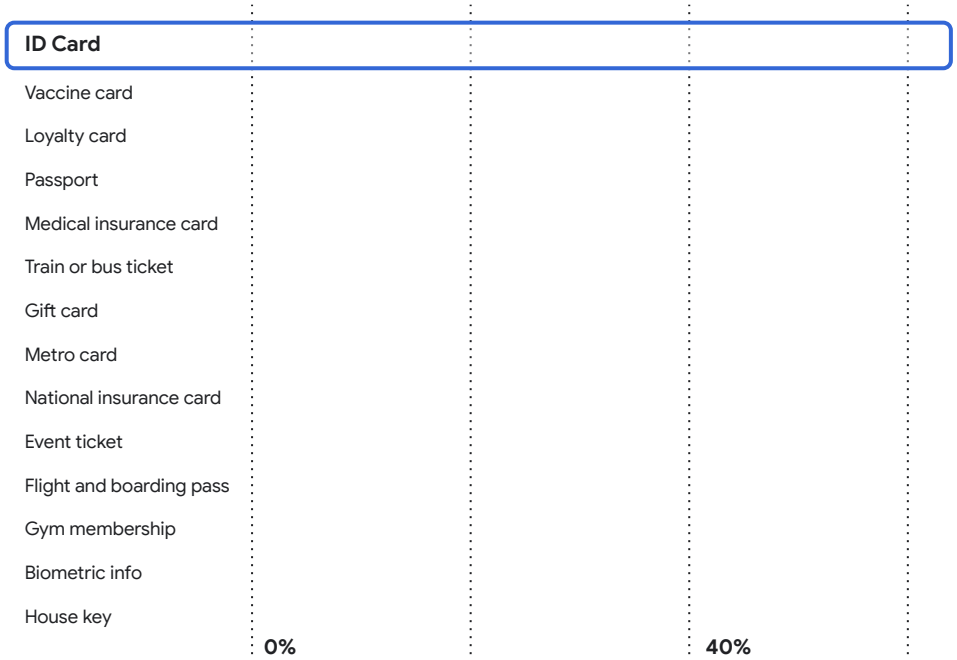
80+

Countries live today with plans to expand globally

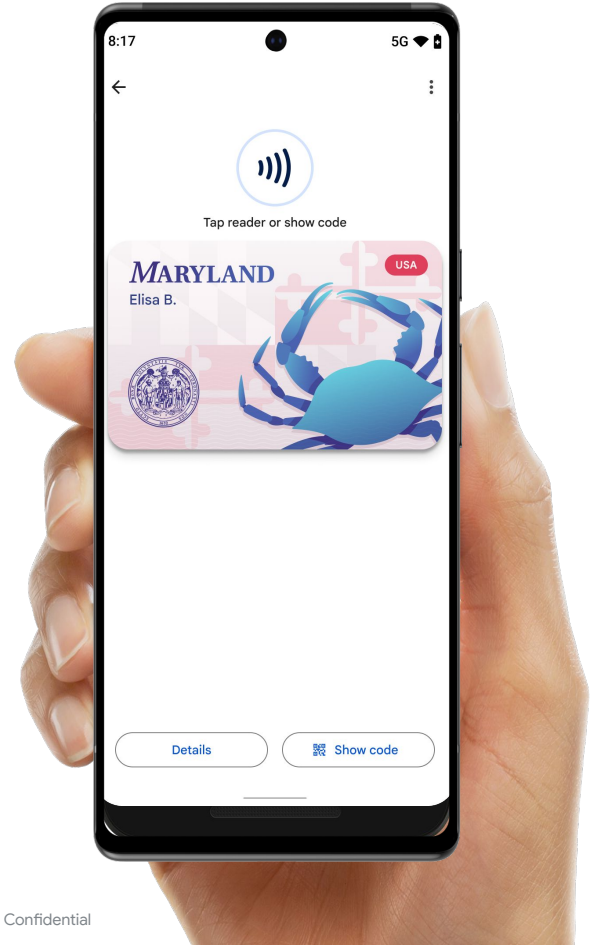
Users list ID Cards as the #1 wallet item they would like digitized.

What items do you wish could be digitized?

Surveys across US, UK, JP, RU, BR, FR



Digital IDs in Google Wallet: Secure and seamless.



Trusted secure data

Data is verified against an authoritative source, digitally signed to mitigate tampering, and stored encrypted only accessible by the user.

Easy to use

Sharing ID is as simple as reviewing requested data and authenticating to share.

Interoperable

Collaborated with industry stakeholders to define ISO standards for digital IDs to ensure ease of developer adoption and an open ecosystem.

Android Security

Security Primitives in Android for ID apps

- **Verified Boot, OS immutability, and signed sandboxed applications**
  - Provides guarantees to the ID issuer that all code being executed on a device is from a trusted source (device manufacturer, application vendor, etc)

- **Availability of hardware-backed cryptography**
  - Elliptic Curve Cryptography
    - P-256 ECDSA on essentially all devices
    - P-256 ECDH, Ed25519, X25519 on newer devices
  - Optional limited number of uses per key
  - User Authentication (LSKF and/or biometric)
  - Attestation of hardware-backed keys, including device-claims about Verified Boot
  - Private key material is designed to never leave the Secure Area (TEE or SE)
  - StrongBox-variant for devices with certified Secure Elements
  - Secure Key Import on newer devices (for keys generated off-device)

- **OMAPI for communication with Secure Elements on devices that have them**
  - Albeit in a fragmentation-prone way

- **Our OWF Identity Credential stack is built on top of this foundation**

Thank You