Passkeys vs. Verifiable Digital Credentials **Friends or Foes?**

Tim Cappalli

authenticate 2025
THE FIDO CONFERENCE

Signature Sponsors
Google | Microsoft | VISA | yubico

Quick Intro

Identity Standards @ Okta

Digital Credentials

Boston

timcappalli.me

Agenda

- Refresher: What are passkeys and VDCs?
- What are **passkeys** really good at?
- What are **VDCs** really good at?
- Challenges with **VDCs**
- Friends or foes?

this presentation is in the context of

authentication

~~identification~~

~~authorization~~

What are passkeys?


JUST KIDDING!

but…

two important reminders

Passkeys are…

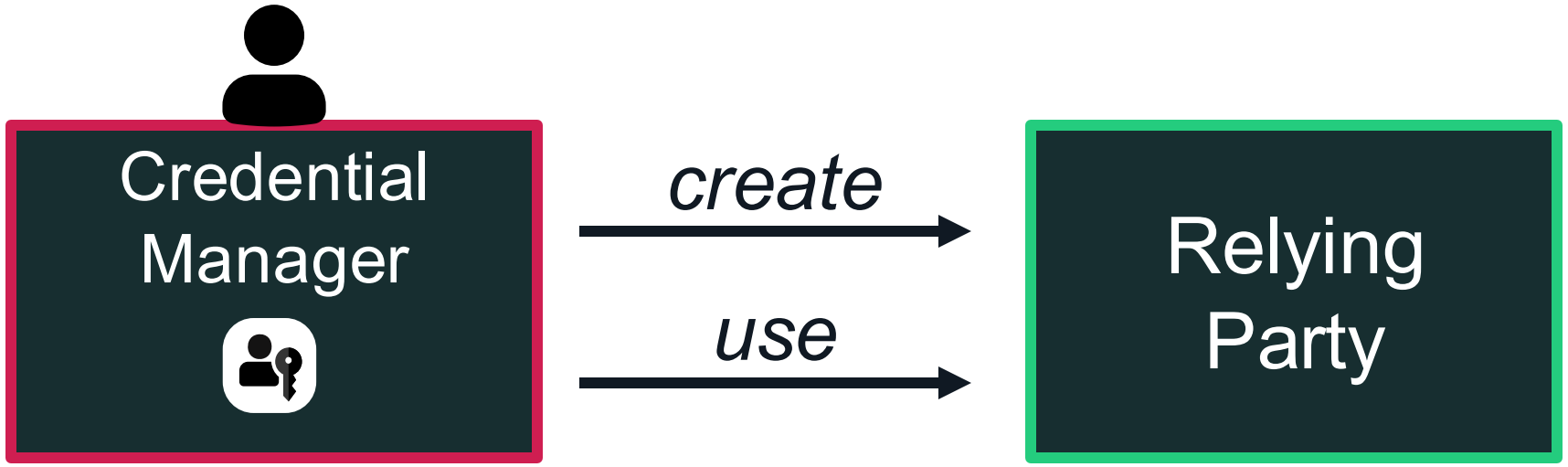
Pairwise

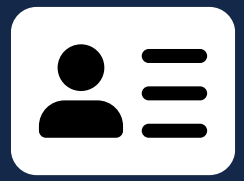
(unique per account + service)

BYOK

(bring your own key)

Bring Your Own Key (BYOK)





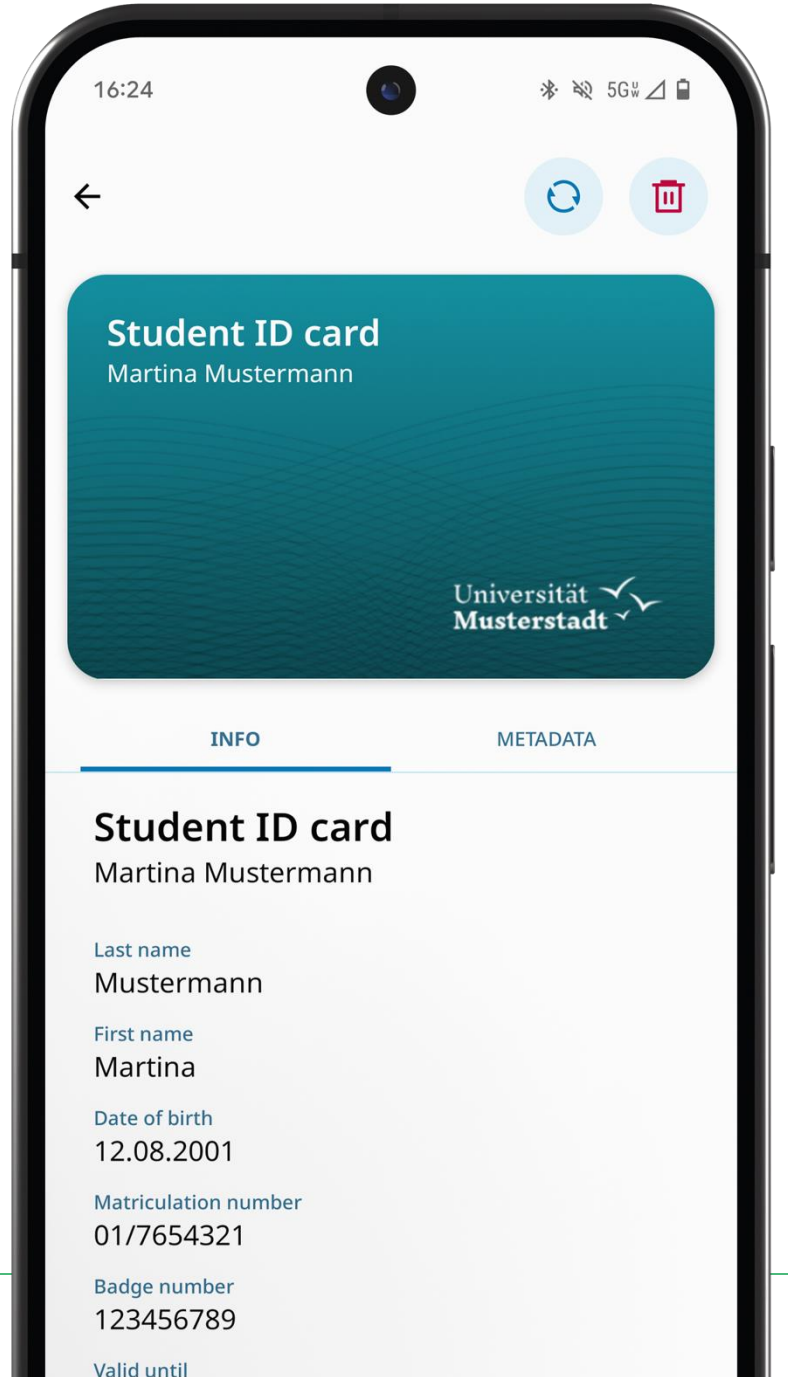
What are verifiable digital credentials?

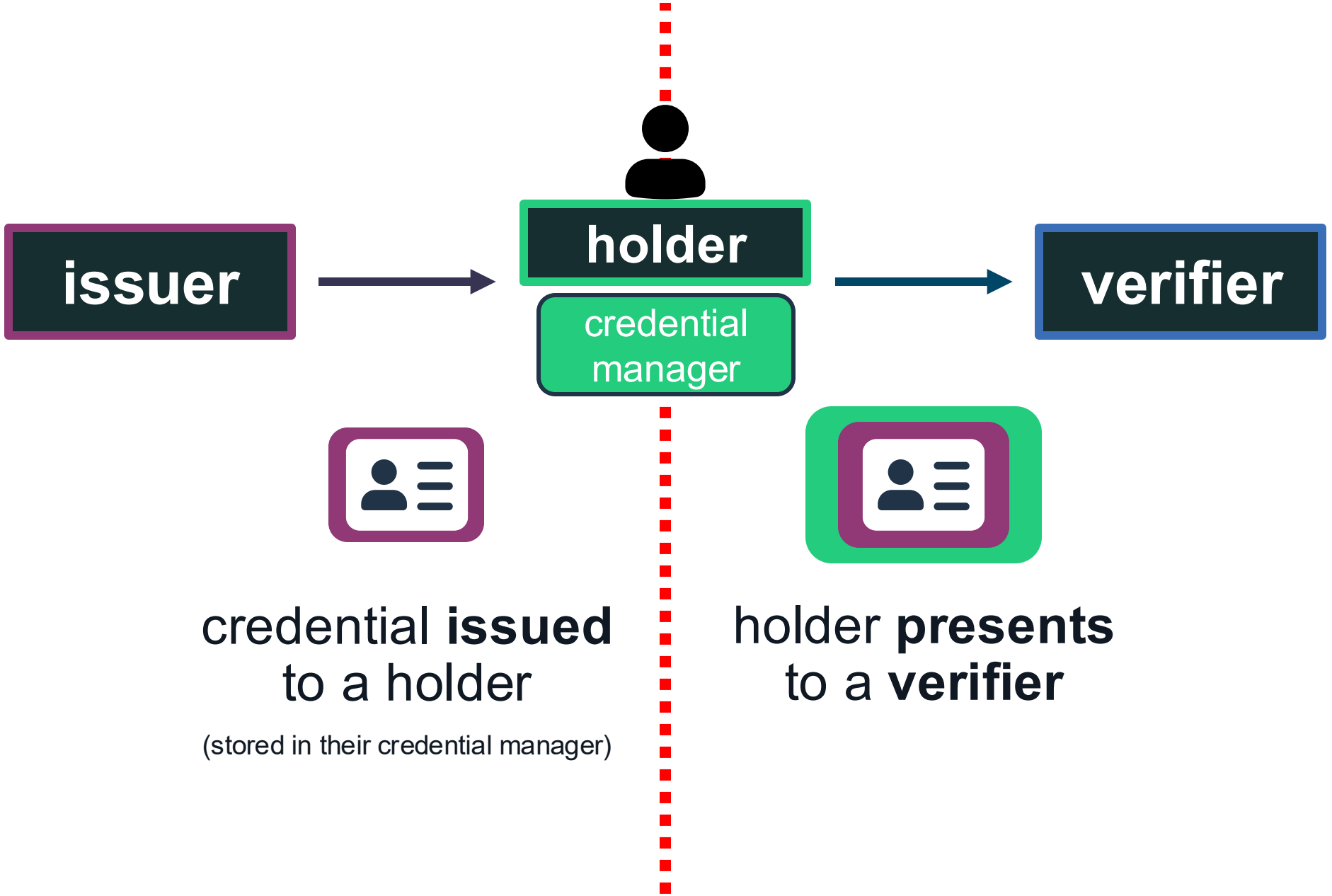
Verifiable Digital Credentials (VDCs)

a set of

issuer-signed

claims




issuer
holder
credential manager
verifier
credential **issued** to a holder
(stored in their credential manager)
holder **presents** to a **verifier**

What are **passkeys** really good at?

Passkeys are really good at…

authenticating users

purpose built for easy, phishing-resistant authentication

they don't do much else (which is a feature!)

Highly and Widely Available

One type,
few parameters

“Create a passkey pls”

```
{
  "challenge": "...718sA",
  "timeout": 60000,
  "rpId": ”login.example.com",
  "userVerification": "preferred"
}
```

Natively supported on nearly every user device in the world

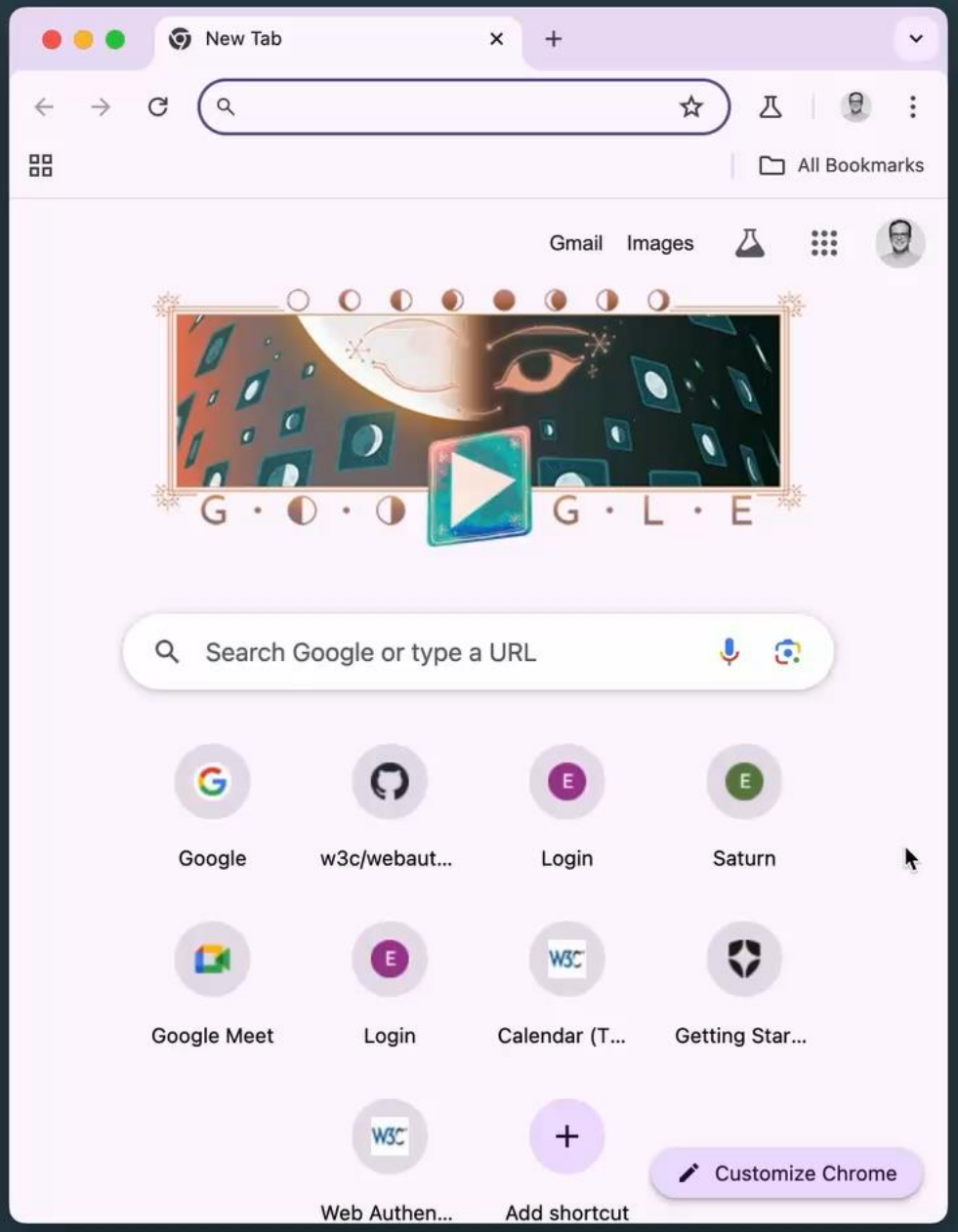
estimate is >95%

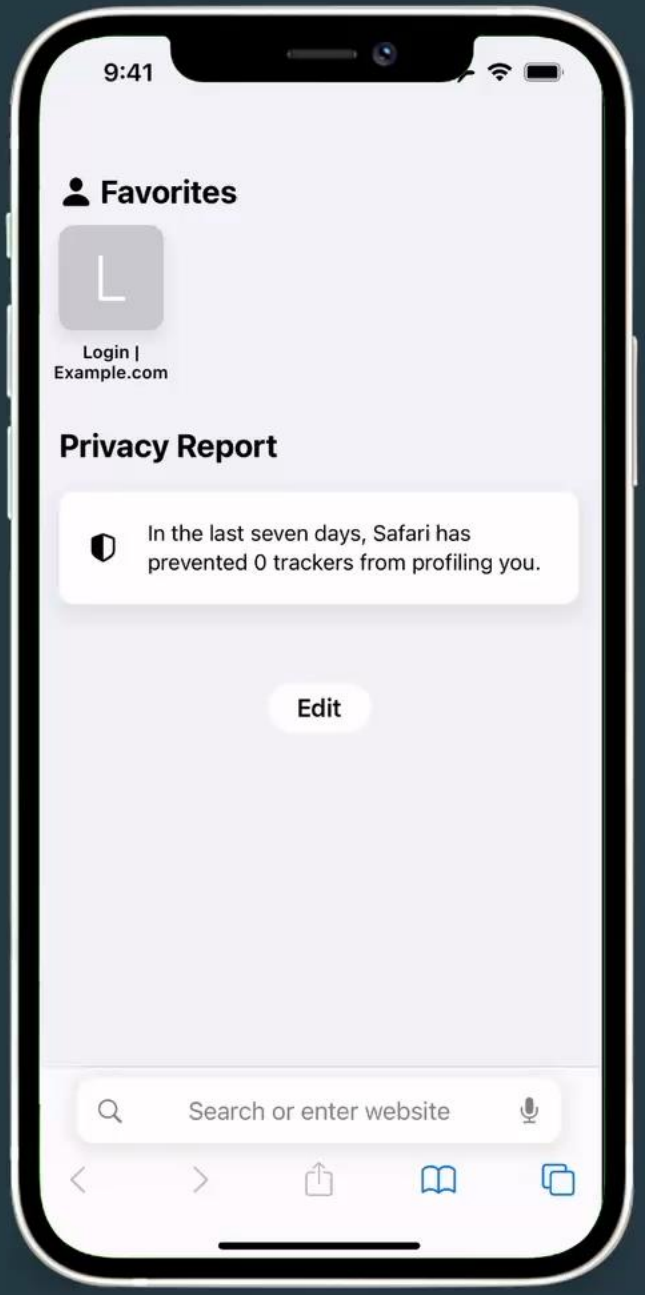
Windows 10+

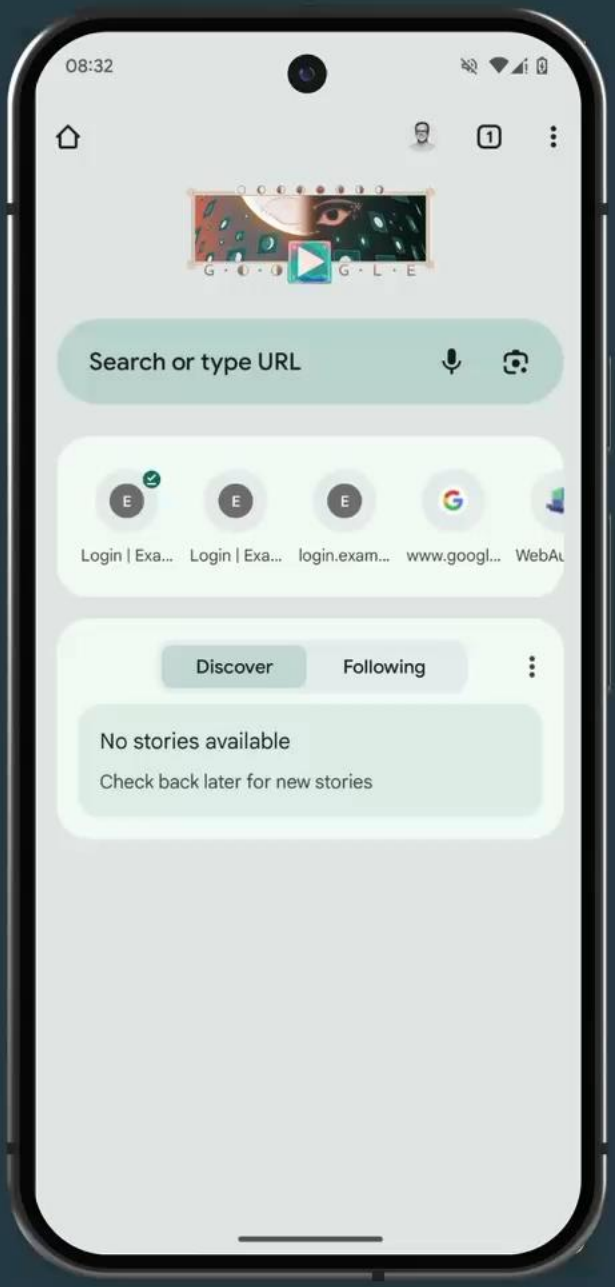
macOS 13+

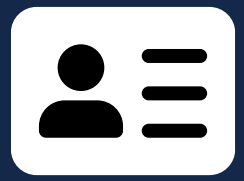
Android 9+

iOS 16+


New Tab
All Bookmarks
Gmail
Images
Search Google or type a URL
Google
w3c/webaut...
Login
Saturn
Google Meet
Login
Calendar (T...
Getting Star...
Web Authen...
Add shortcut
Customize Chrome


9:41
Favorites
L
Login |
Example.com
Privacy Report
In the last seven days, Safari has prevented 0 trackers from profiling you.
Edit
Search or enter website


08:32
Search or type URL
Login | Exa...
Login | Exa...
login.exam...
www.googl...
Discover
Following
No stories available
Check back later for new stories



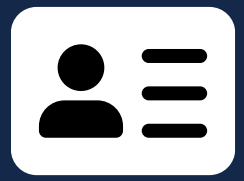
What are **verifiable digital credentials** really good at?

VDCs are really good at…

empowering users to control what identity data they share

(typically for identification or authorization)

purpose built for user-centric control



Challenges with verifiable digital credentials

18013-7 Annex D

18013-7 Annex B

OpenID4VP

Custom Schemes

VC API

SD-JWT

W3C VC DM

18013-7 Annex C

DIDComm

Digital Credentials API

SD-CWT

mdoc

AnonCred

18013-7 Annex A

OpenID4VCI

Many Components

Credential formats

Presentation protocols

Issuance protocols

Transports

Schema / Type

Key types

Signature formats

Encryption methods

Availability

Given the various formats, transports, engagement methods, and protocols, it's unlikely a user will have the right credential manager already installed.

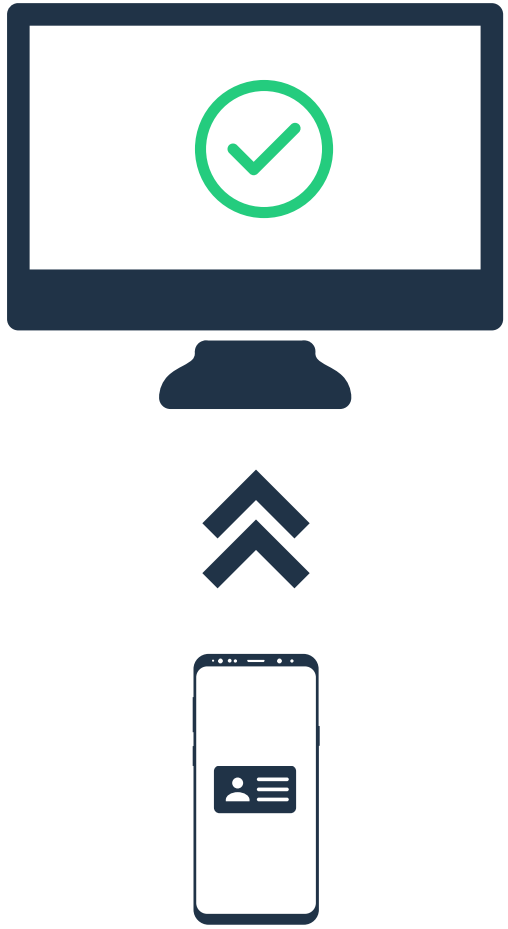
(short to medium term)

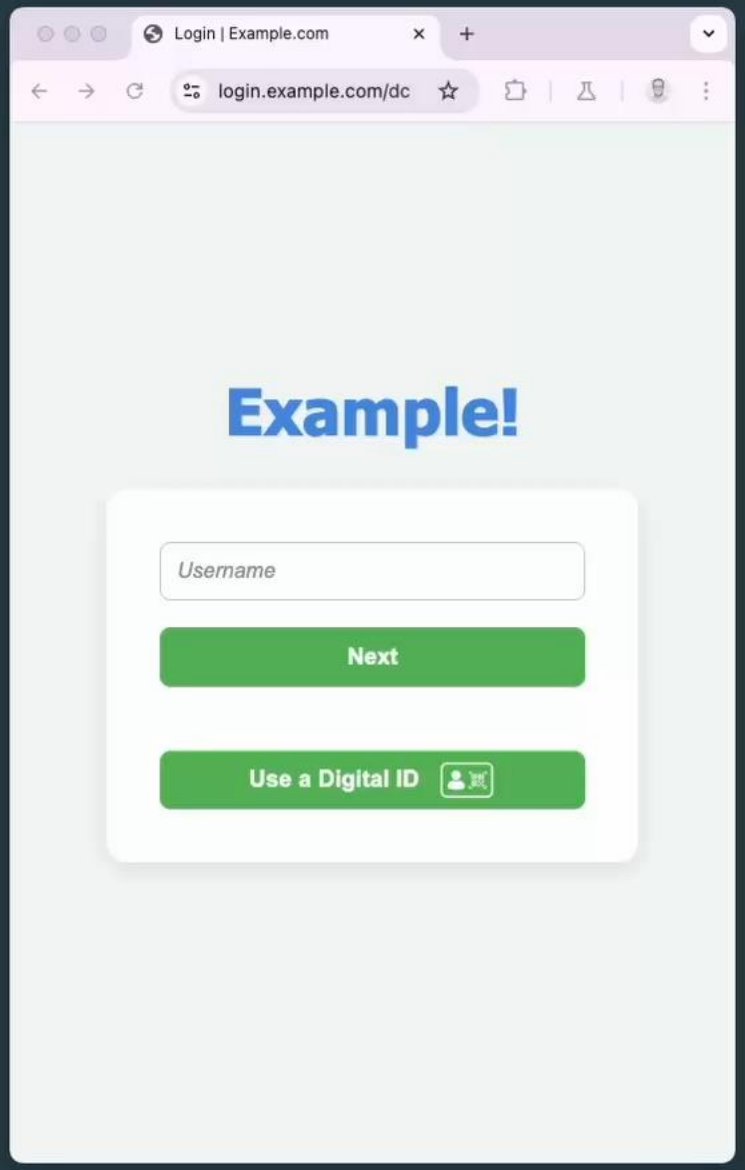
Availability

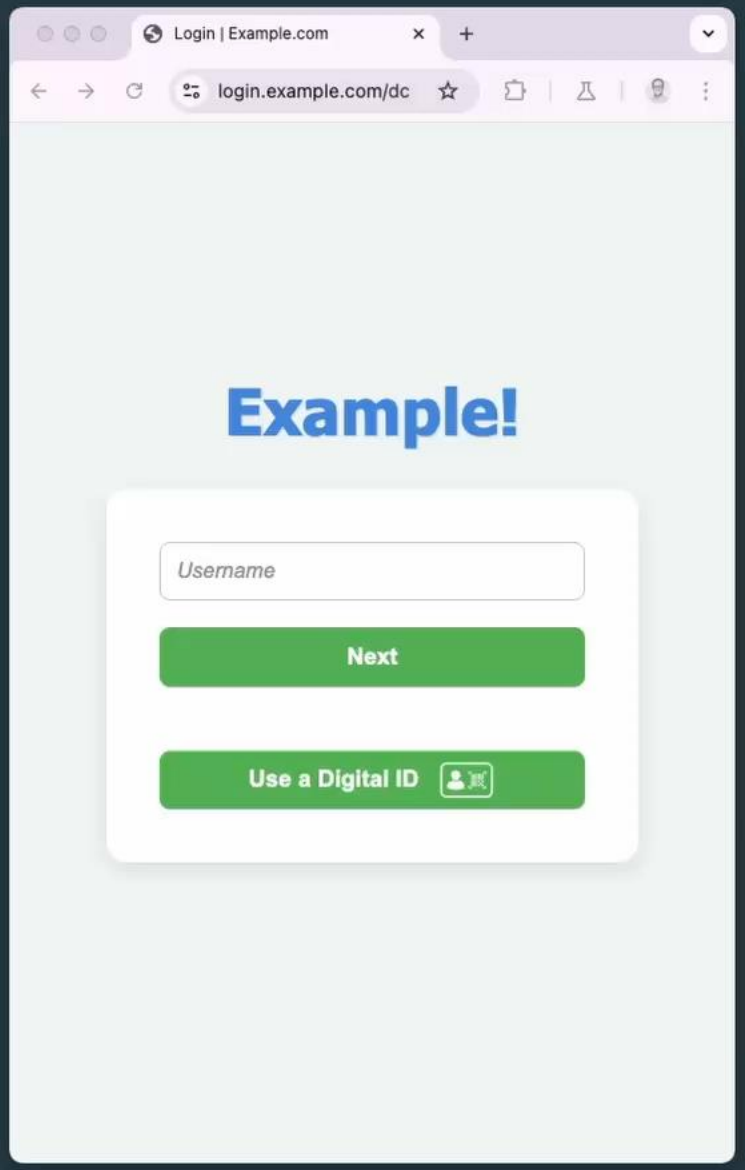
VDCs are currently, and likely to remain, mobile-centric in the short to medium term

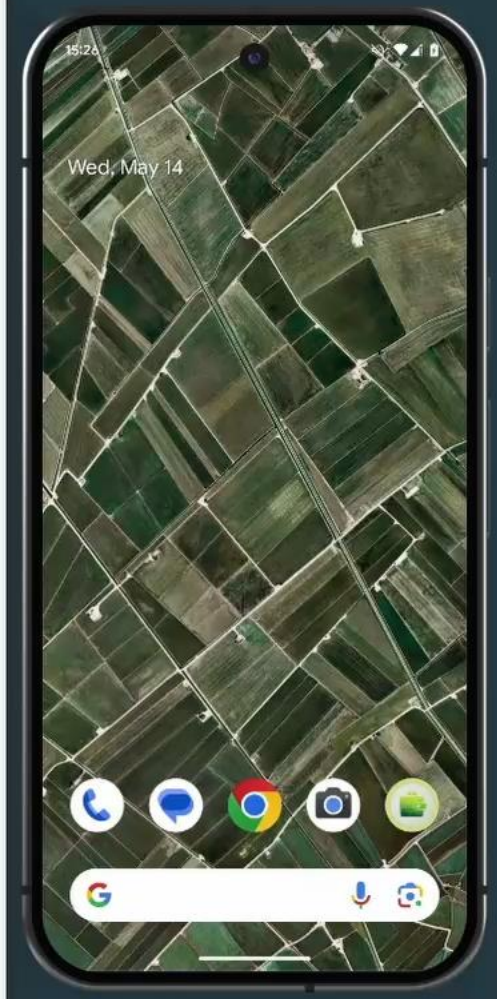
(especially for medium to high assurance credentials)

Cross-device flows are needed for laptops/desktops, which have tested poorly for regular use with users for passkeys.



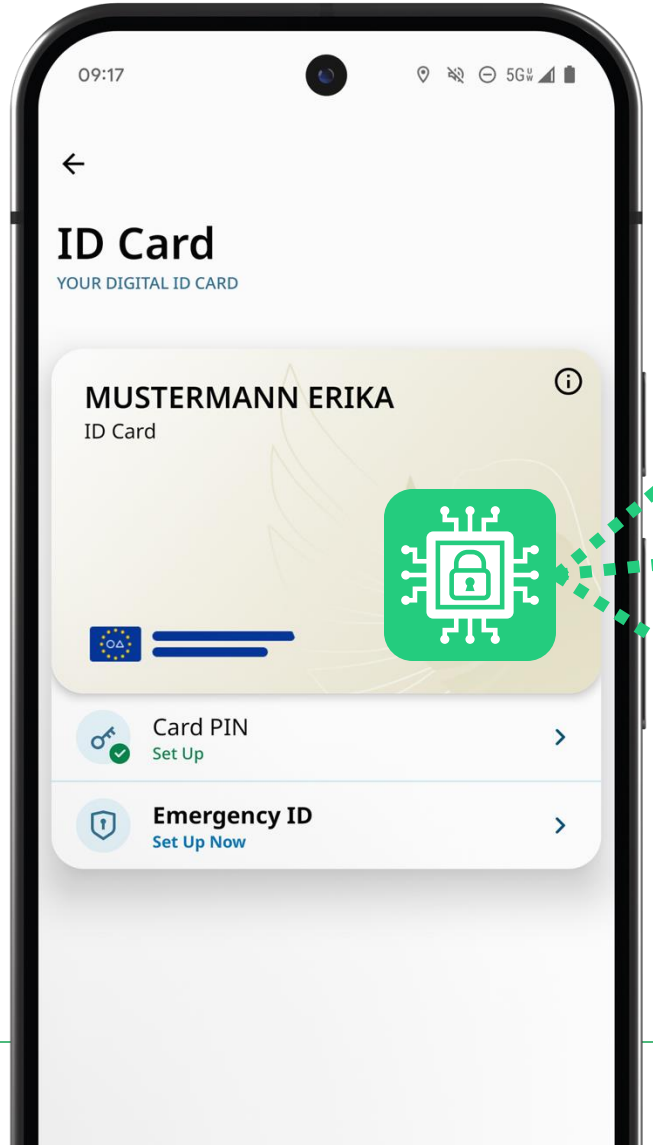

Login | Example.com
login.example.com/dc
Example!
Username
Next
Use a Digital ID

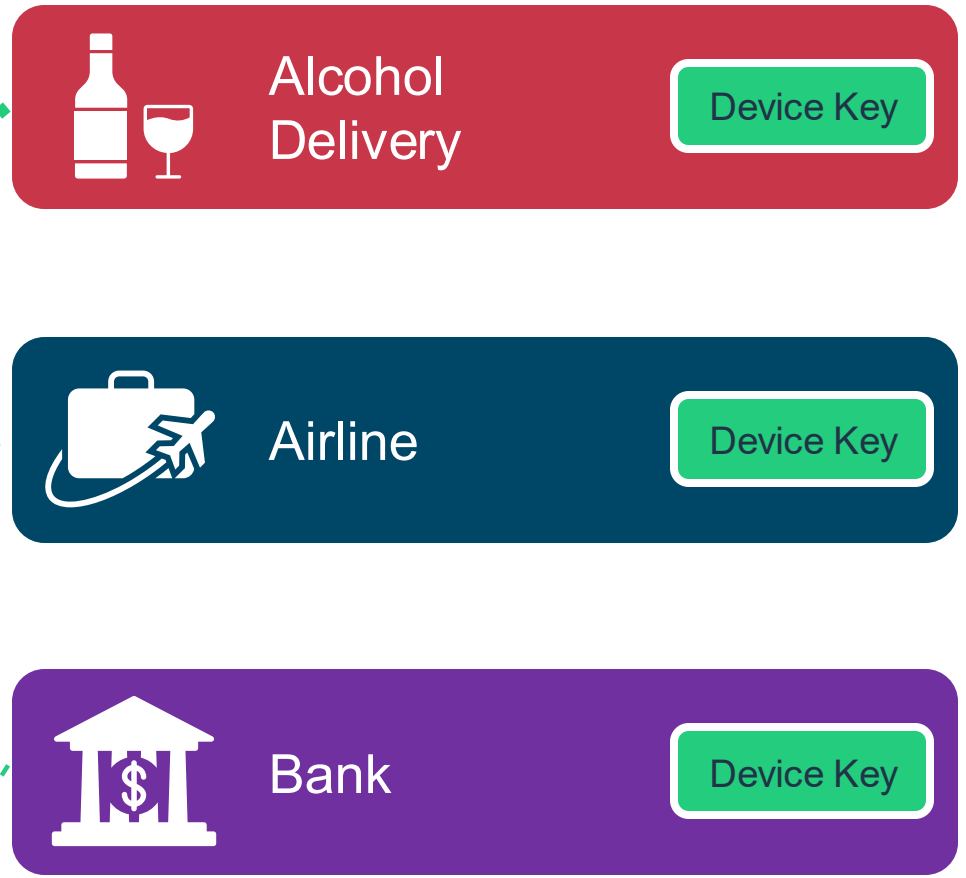

Login | Example.com
login.example.com/dc
Example!
Username
Next
Use a Digital ID


15:26
Wed, May 14

PRIVACY

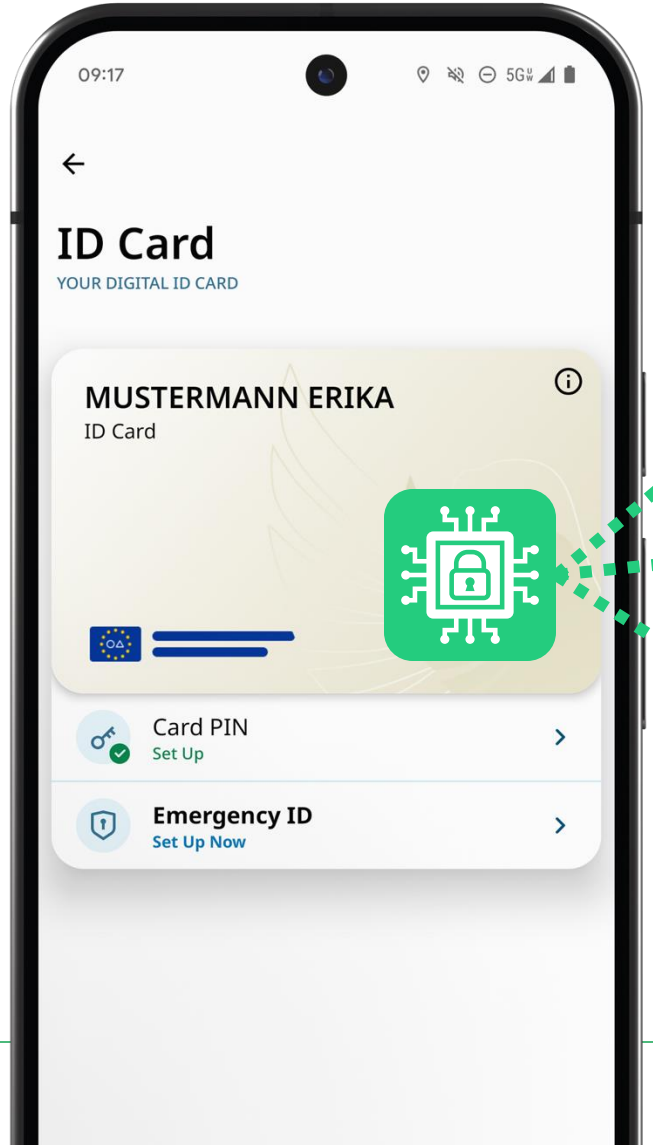
VDCs as a "Super Cookie"





PRIVACY

VDCs as a "Super Cookie"



Potential Solutions

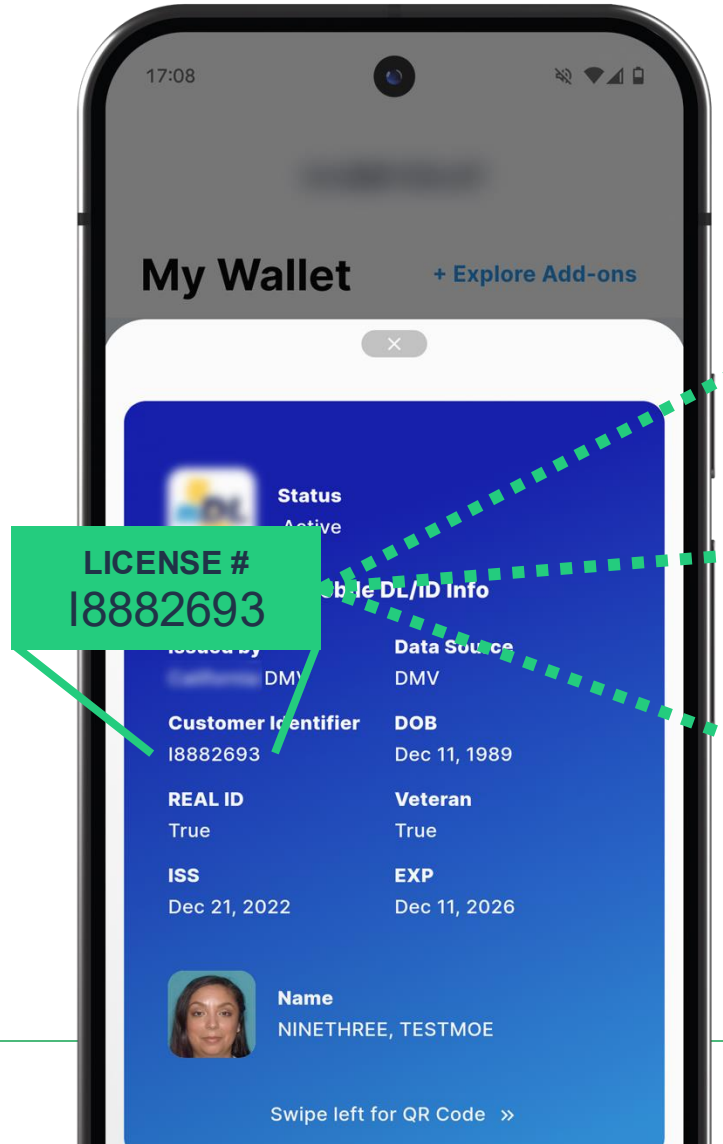
Bulk Issuance
(expensive)

Zero Knowledge Proofs
(still very new, doesn't solve everything)

COLLUSION

PRIVACY

VDCs as a "Super Cookie"



LICENSE #
I8882693

Alcohol Delivery — License #

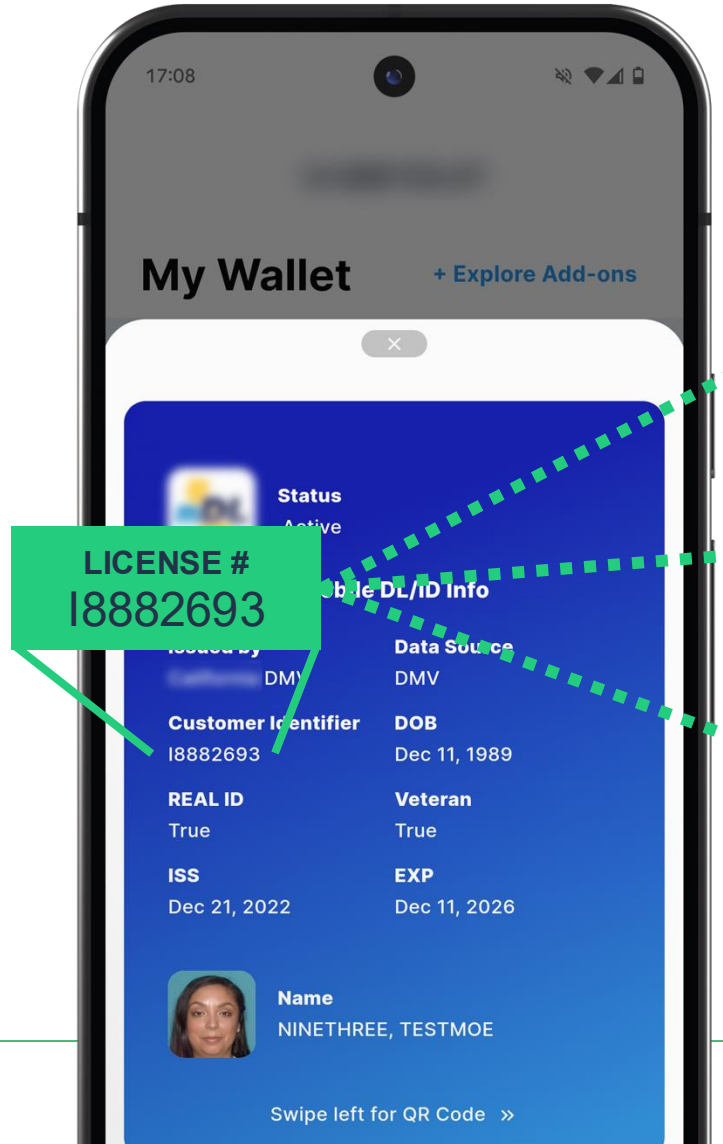
Airline — License #

Bank — License #

COLLUSION

PRIVACY

VDCs as a "Super Cookie"



Potential Solutions

Selective Disclosure
(requires user to understand impact)

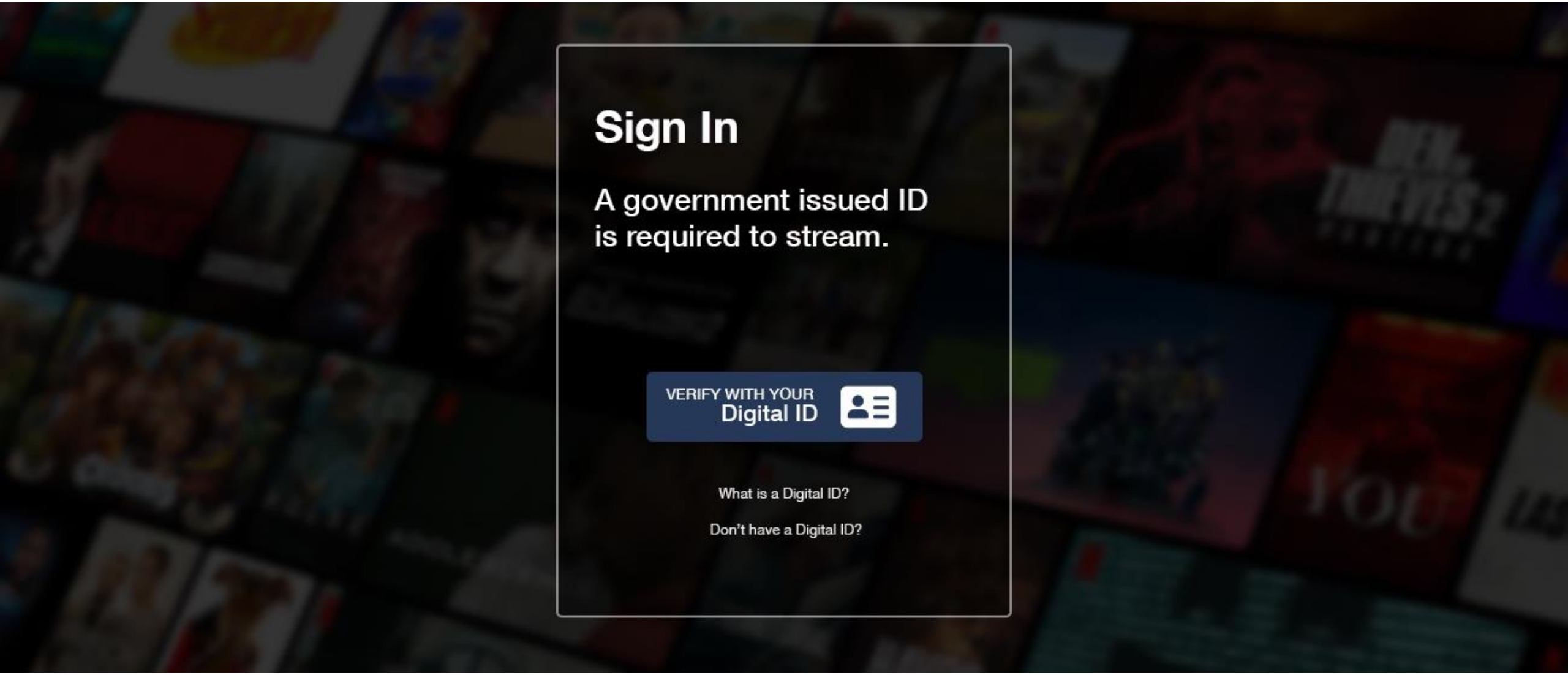
Verifier Registration & Policy/Legal
(challenging in some geos)

Zero Knowledge Proofs & Pseudonyms
(still very new)

COLLUSION

PRIVACY

"Show Your Papers" Web



Friends or Foes?

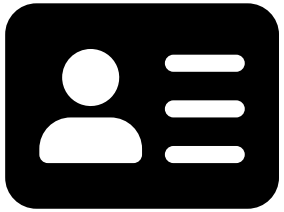
Consumer

federation -or- VDCs

sign up

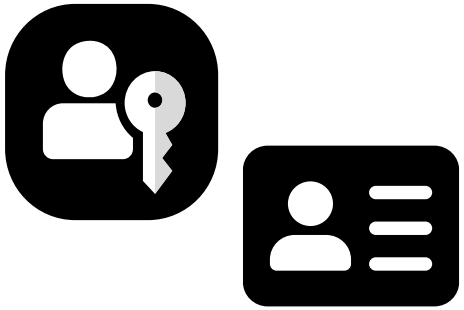
passkeys

sign in



VDCs

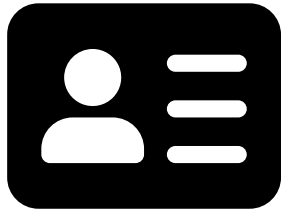
proof up



federation -or- VDCs

recovery

Workforce (employees & contractors)



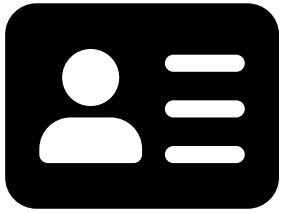
VDCs

~~**sign up**~~

onboard

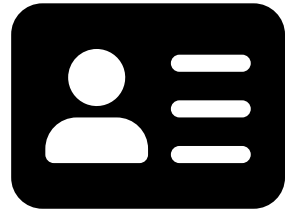
passkeys

sign in



VDCs

proof up



VDCs

recovery

Summary

Passkeys for privacy preserving authentication!

VDCs for user-controlled claims presentment!

Friends not *foes*!

Q&A

Thanks!

connect with me @ timcappalli.me