Passkeys & Verifiable Digital Credentials: Friends or Foes?

Tim Cappalli

@timcappalli.me

Quick Intro

Identity Standards @ Okta

Digital Credentials

Boston

timcappalli.me

Agenda

- Refresher: what are passkeys and VDCs?
- What are **passkeys** are really good at?
- What are **VDCs** are really good at?
- Challenges with VDCs
- Bringing them together

REFRESHER

What are passkeys?

What is a passkey?

public / private key pair

phishing-resistant
(verifier name binding)

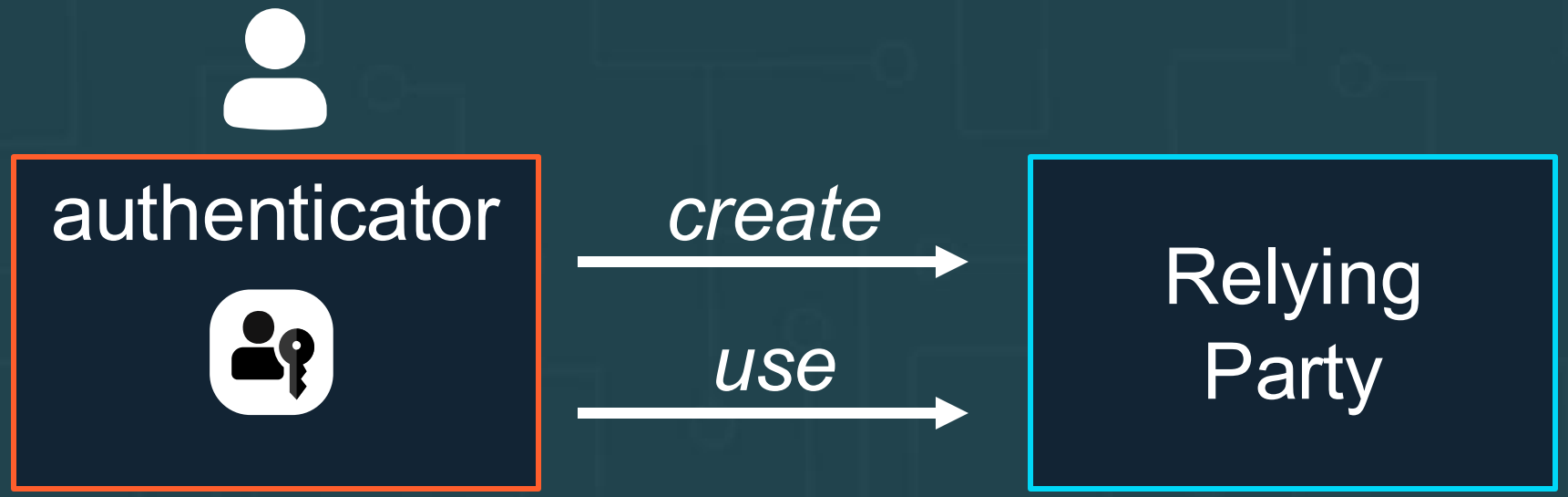
standards-based

pairwise
(unique per account + service)

device-bound or **synced**
(synced available by default)

used via the **WebAuthn** API
(and platform native interfaces)

What is a passkey?



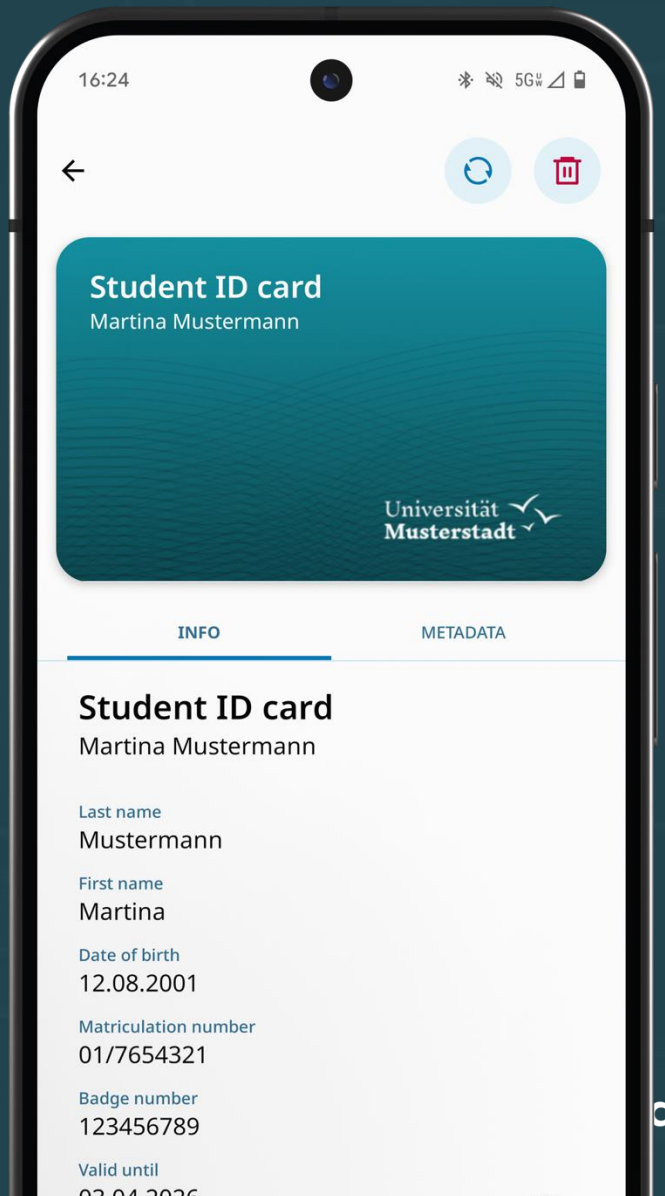
REFRESHER

What are verifiable digital credentials?

Verifiable Digital Credentials

fundamentally a

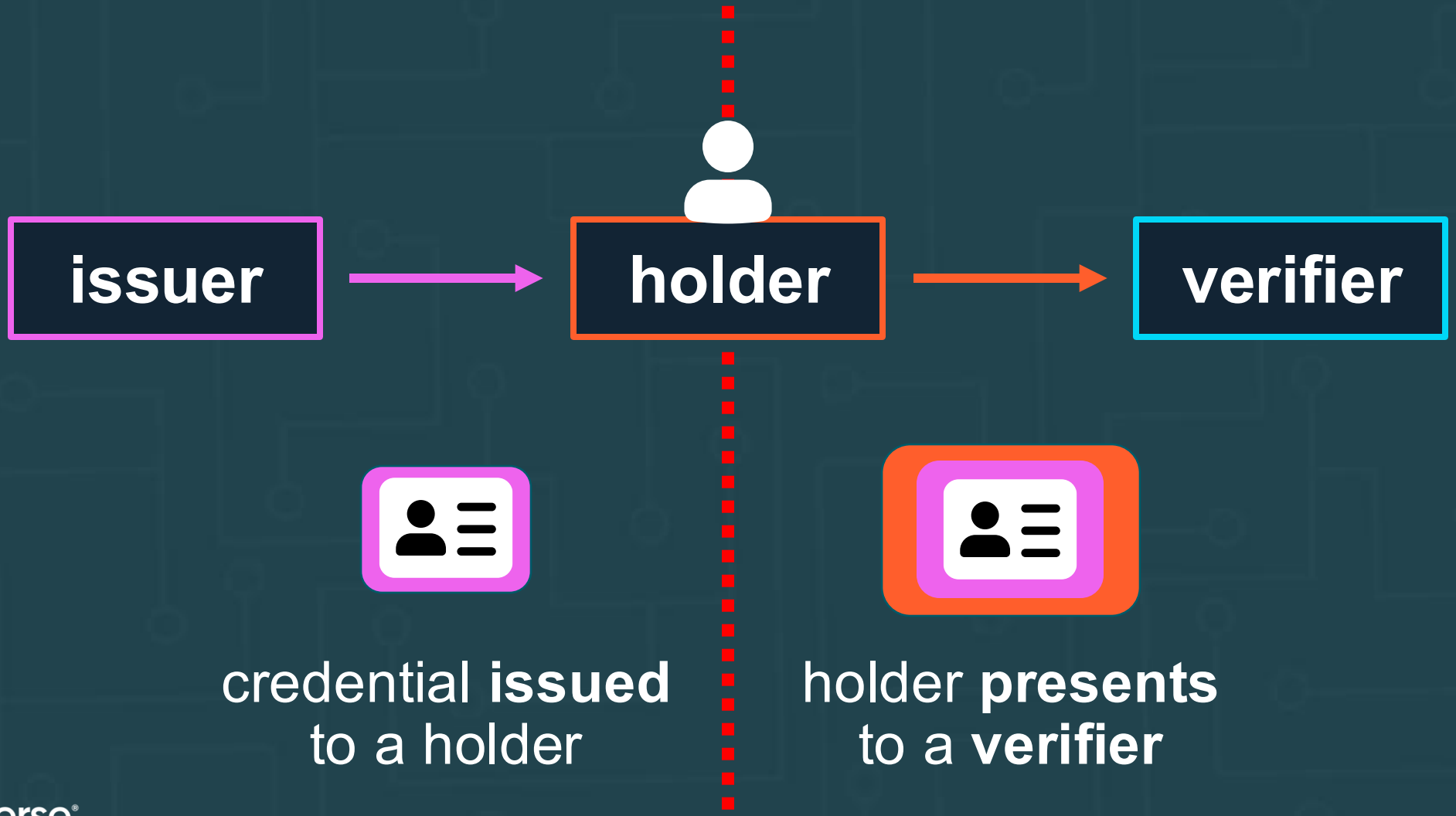
signed set of claims



identiverse®

identiverse

Verifiable Digital Credentials



Trending Types

Government Identity

Driving License

eID

Passport

Travel Documents

Boarding Pass

Visa

Authorizations

Proof of

Employment

Education

Certification

Income

Insurance

What are **passkeys** really good at?

Passkeys are really good at…

authenticating users

purpose built for authentication

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

Availability

One type,
few parameters

“Give me a passkey pls”

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

Natively supported on nearly every user device in the world

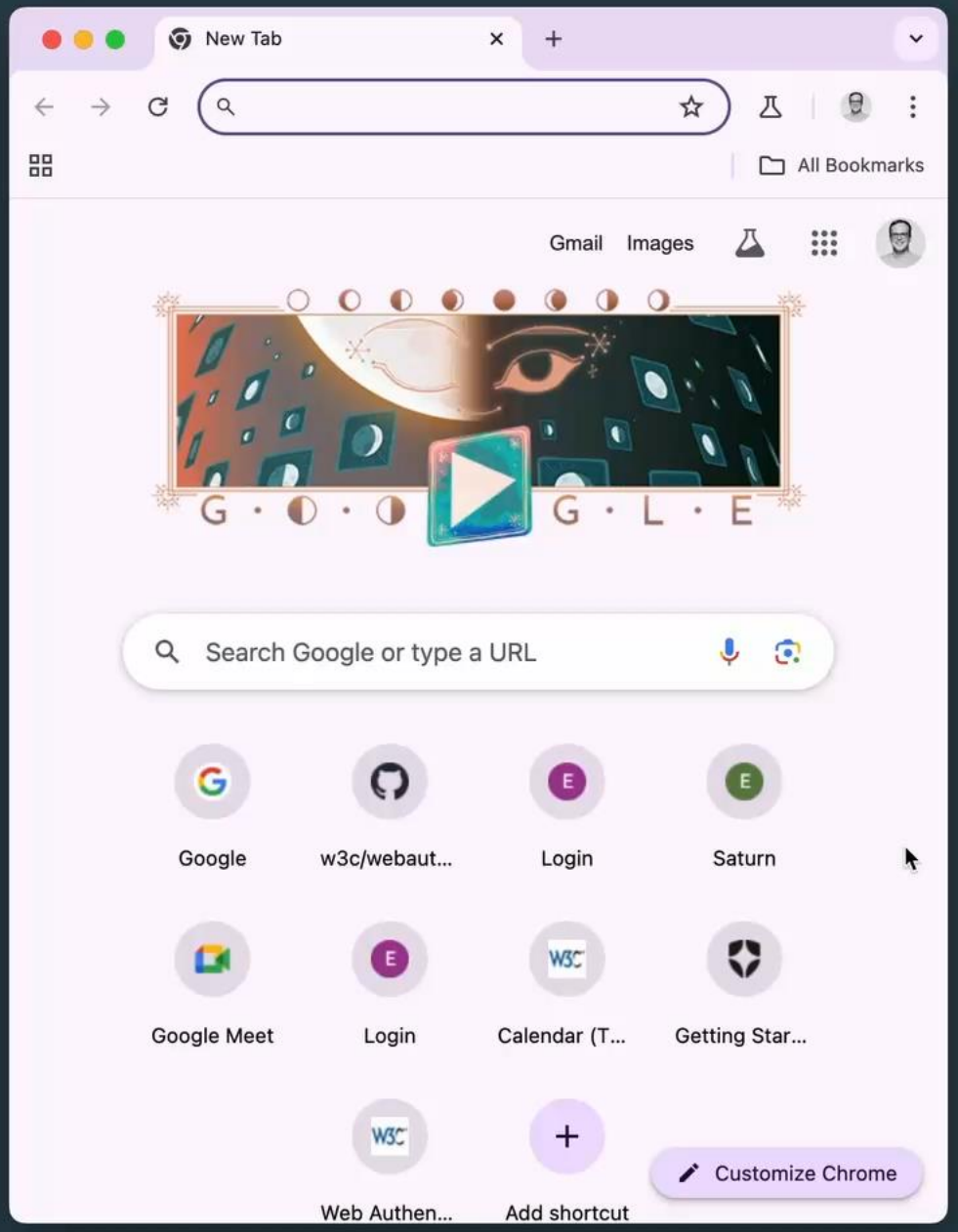
estimate is >95%

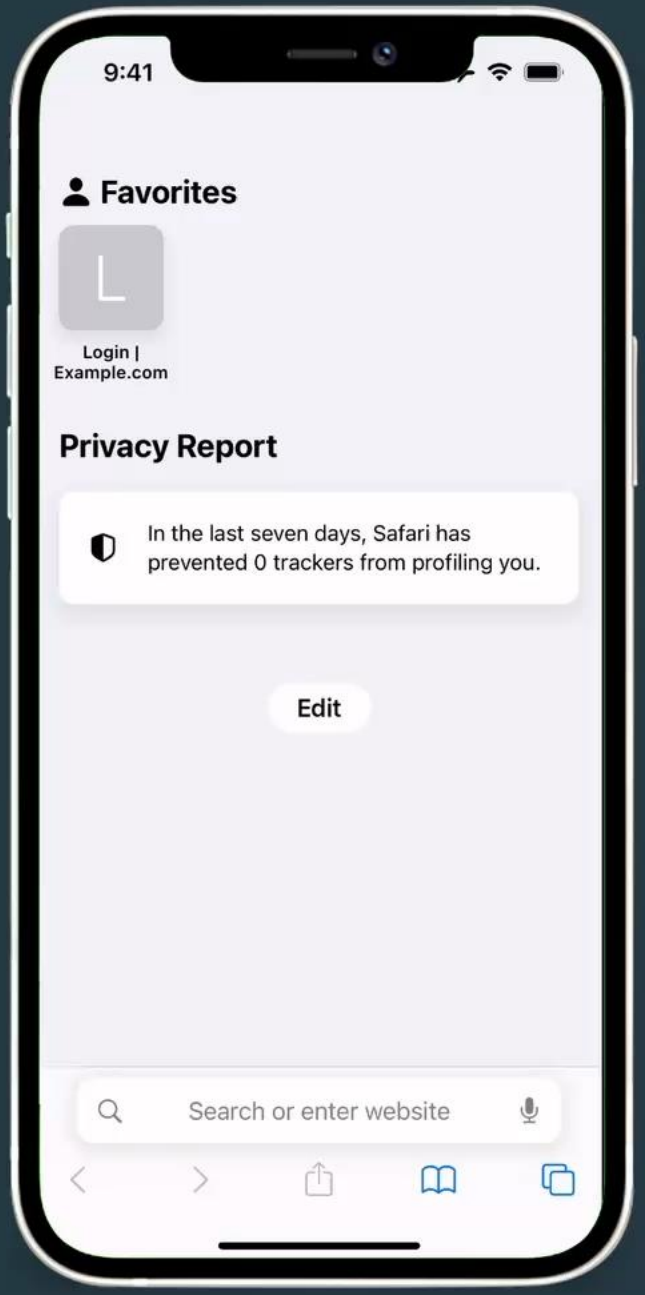
Windows 10+

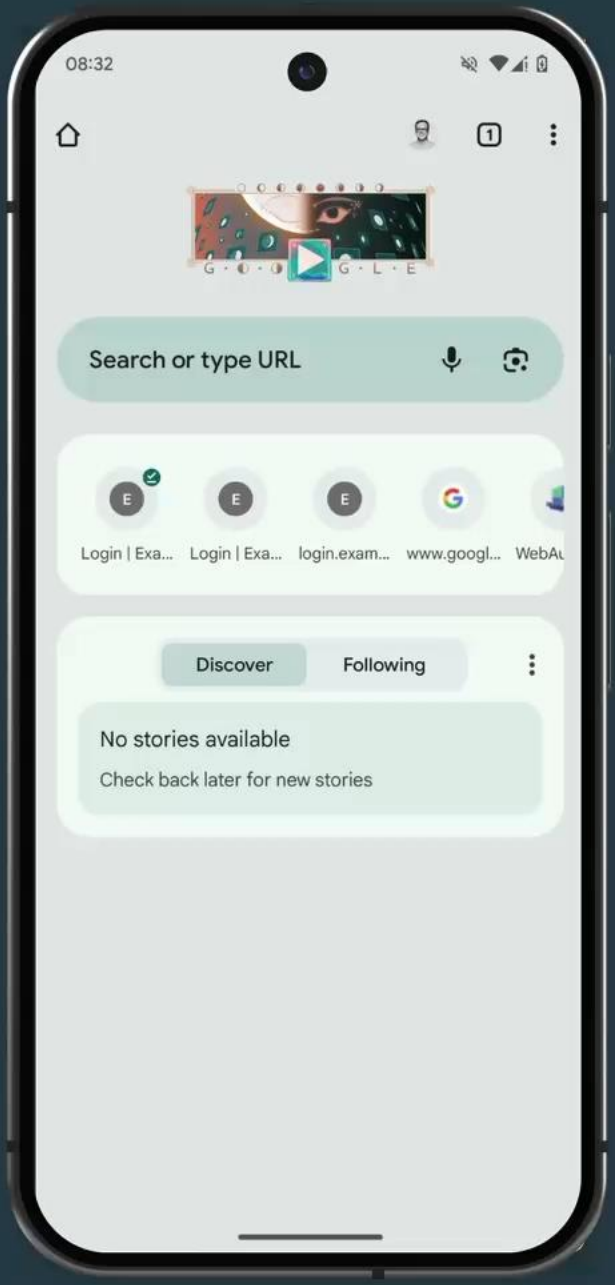
macOS 13+

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…

giving users control of identity data disclosure

purpose built for user-centric control

Challenges with verifiable digital credentials

OpenID4VP

18013-7 Annex B

VC API

DIDComm

18013-7 Annex C

SD-JWT

W3C VC DM

mdoc

Digital Credentials API

SD-CWT

AnonCred

18013-7 Annex A

OpenID4VCI

Many Elements

Credential formats

Presentation protocols

Issuance protocols

Transports

Schema / Type

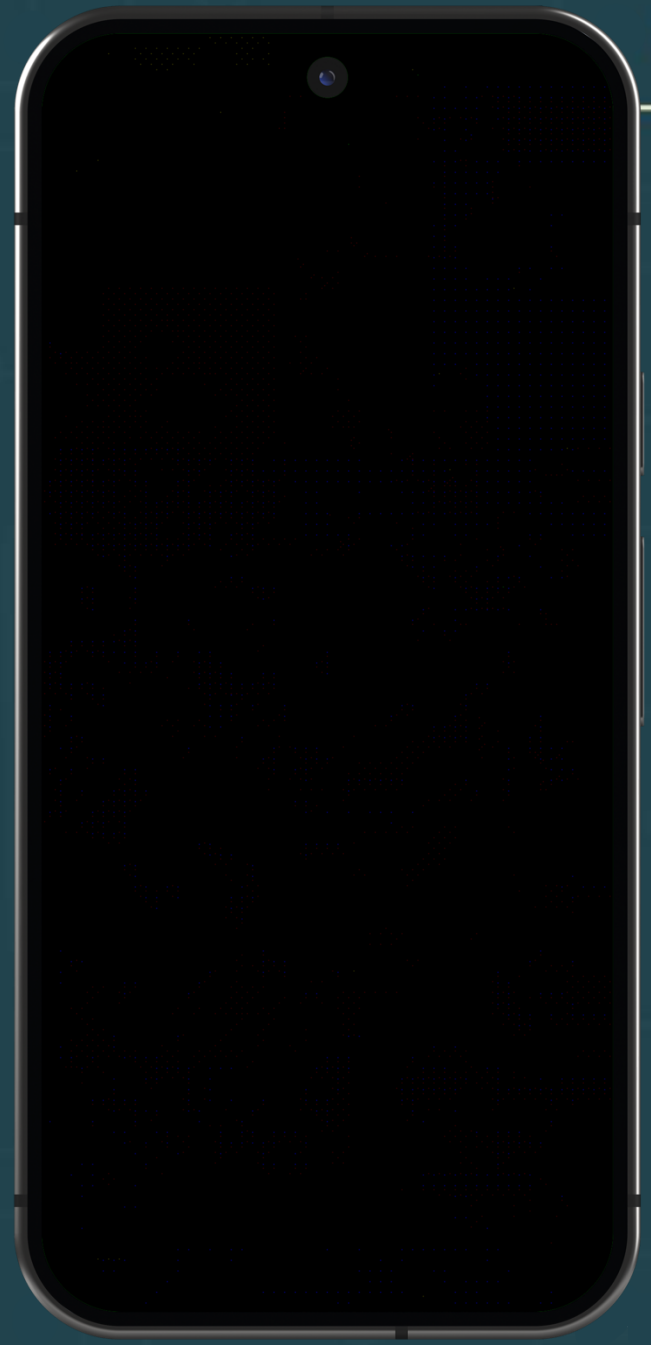
Key types

Signature formats

Encryption methods

Availability

Due to the specific combinations of credential formats, engagement methods, transport protocols, and presentation / issuance protocols, **it's improbable that a user already has a supported credential provider installed and ready**.

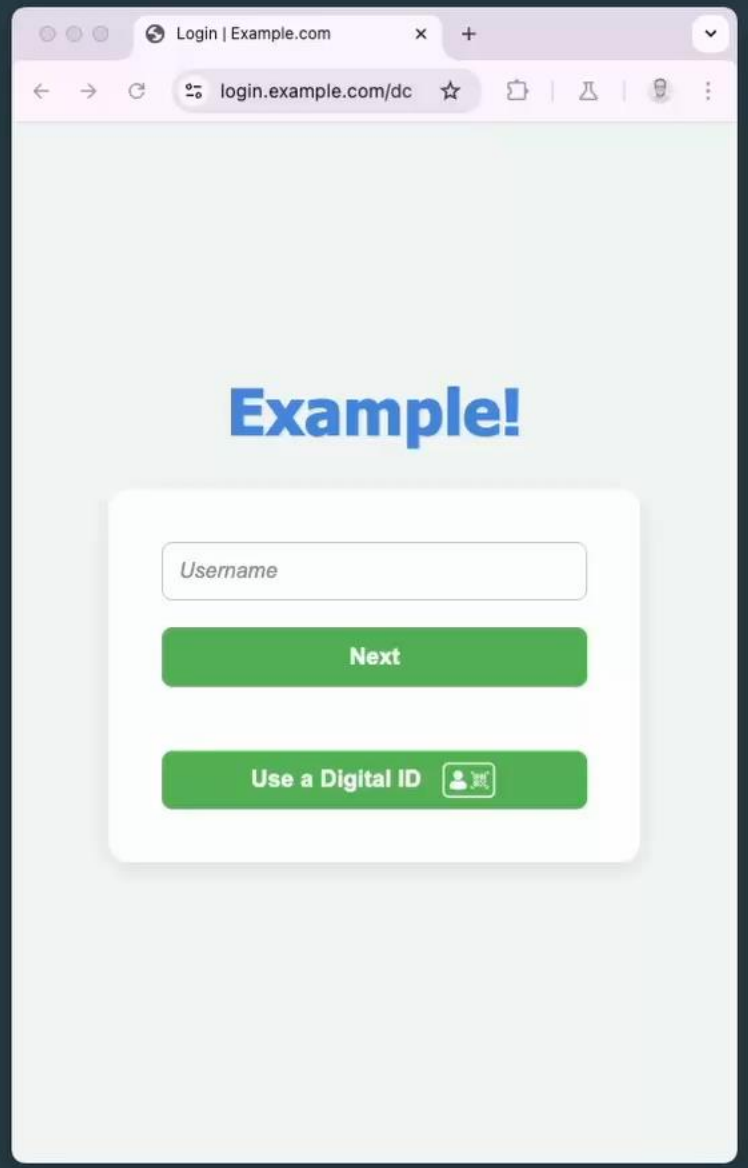


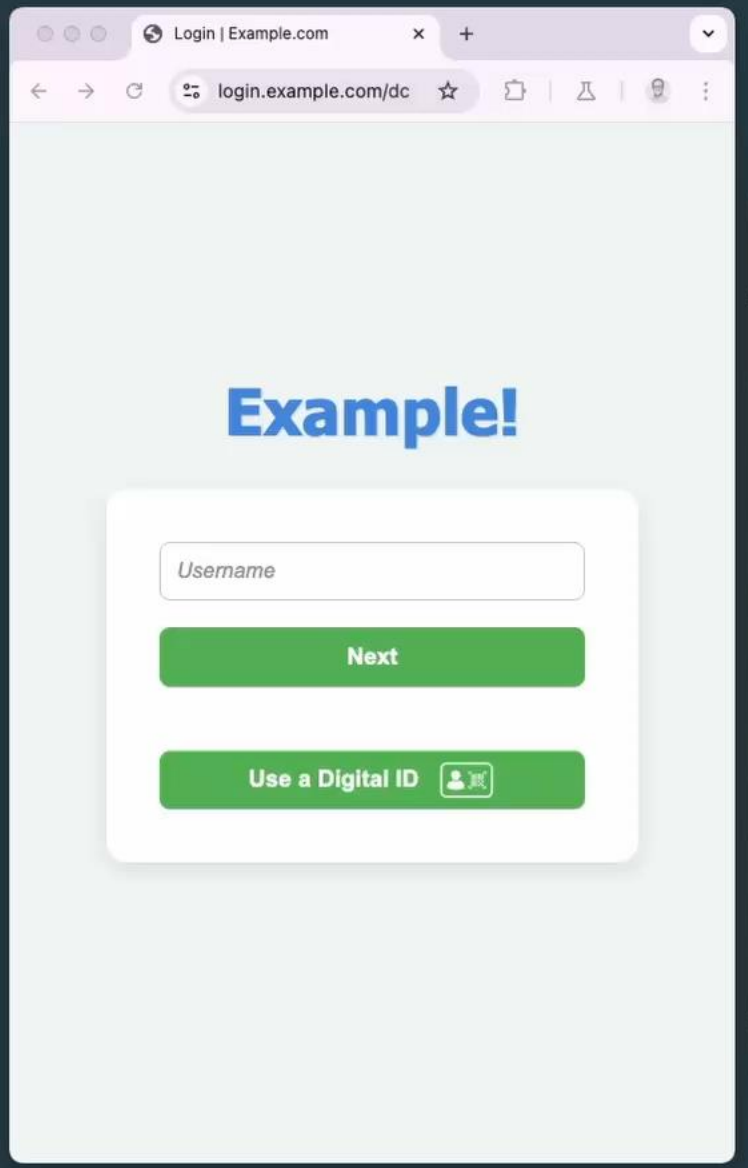
identiverse®

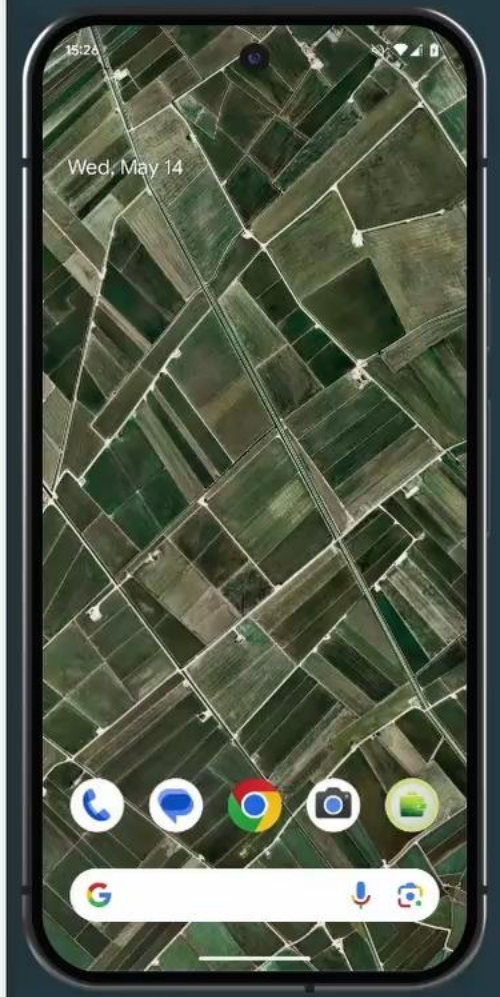
Availability

VDCs are currently, and likely to remain, mobile-centric in the short to medium term (especially for medium to high assurance credentials).

This means cross-device flows are necessary for laptops and desktops, which have tested poorly with users for passkeys.

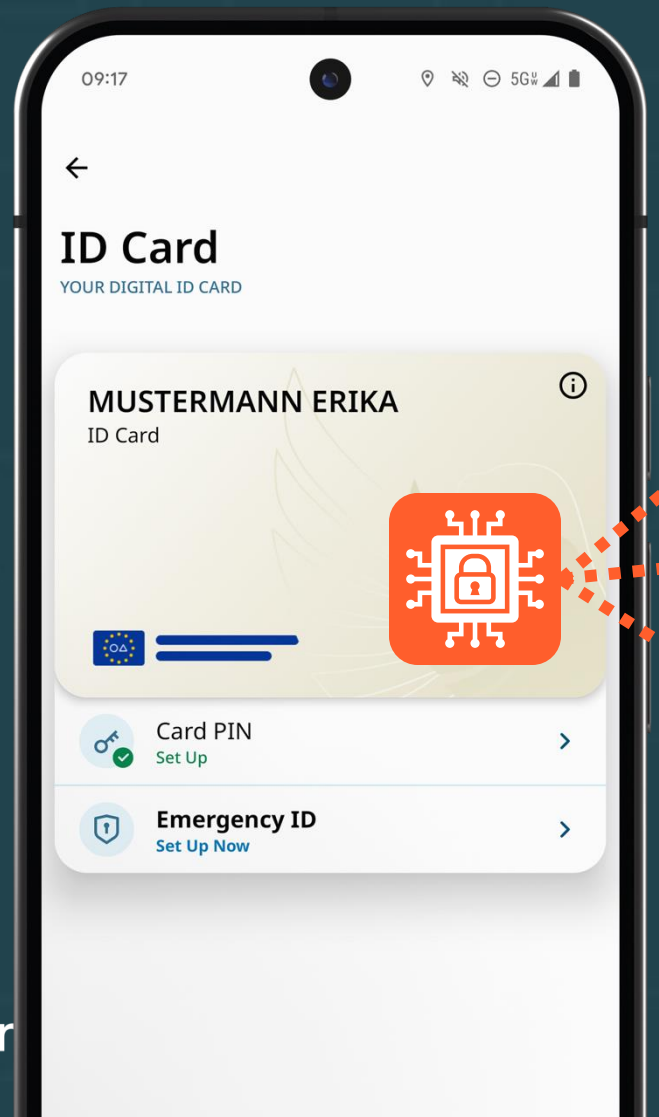

Login | Example.com
login.example.com/dc
Example!
Username
Next
Use a Digital ID


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


Wed, May 14

PRIVACY

VDCs as a Super Cookie



Alcohol Delivery — Device Key

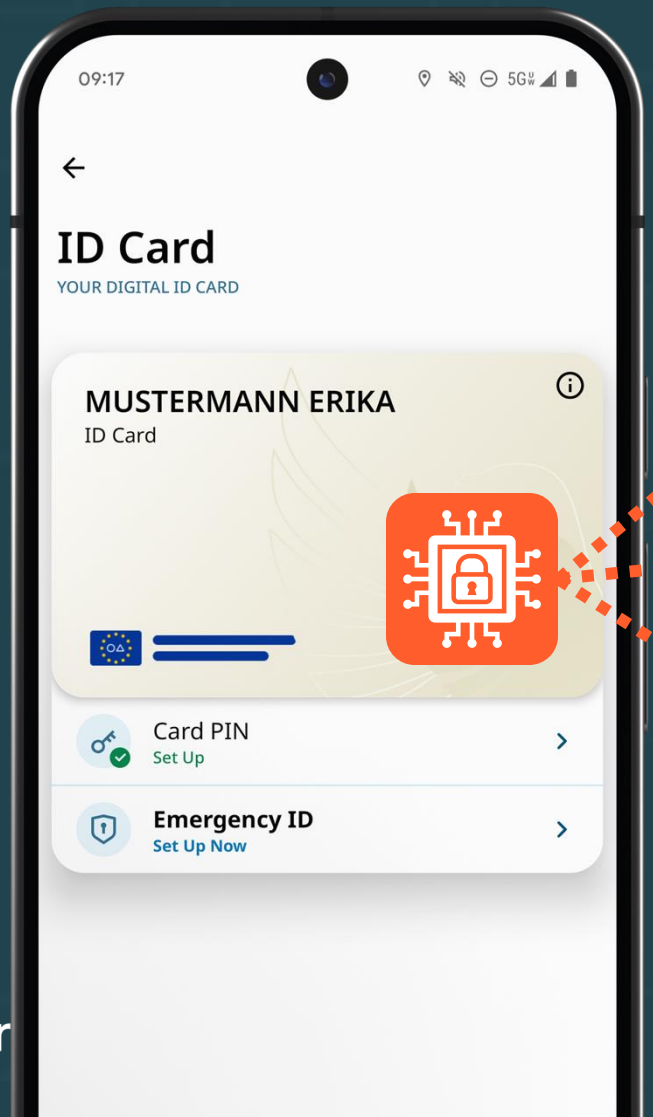
Airline — Device Key

Bank — Device Key

COLLUSION

PRIVACY

VDCs as a Super Cookie



Potential Solutions

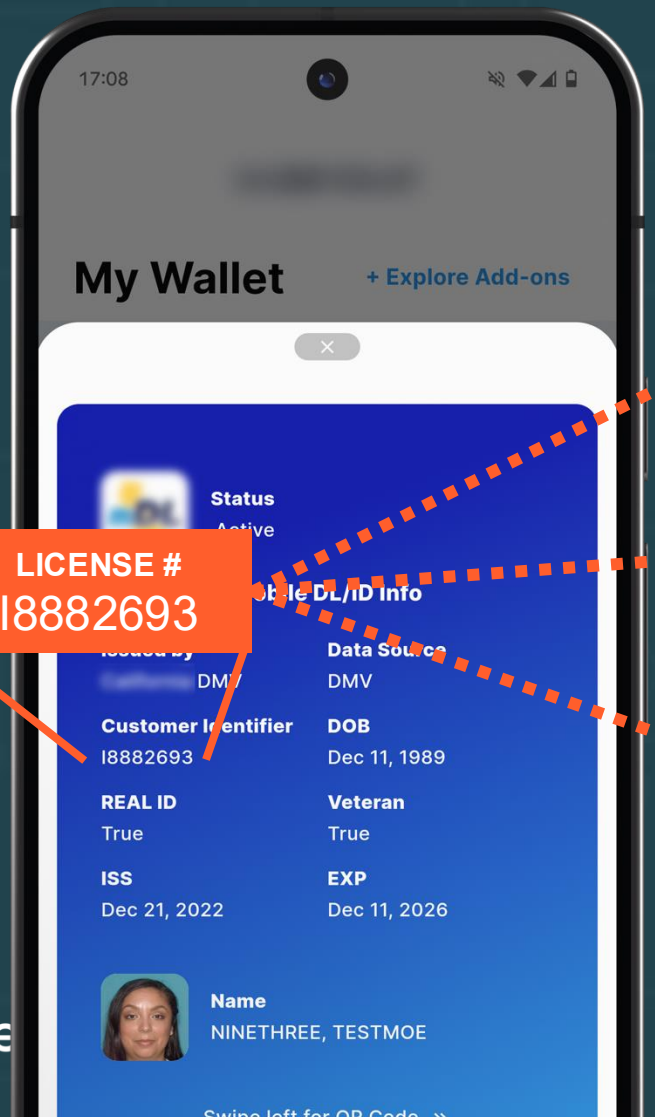
Bulk Issuance
(expensive)

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

COLLUSION

PRIVACY

VDCs as a Super Cookie



LICENSE #
I8882693

Alcohol Delivery — License #

Airline — License #

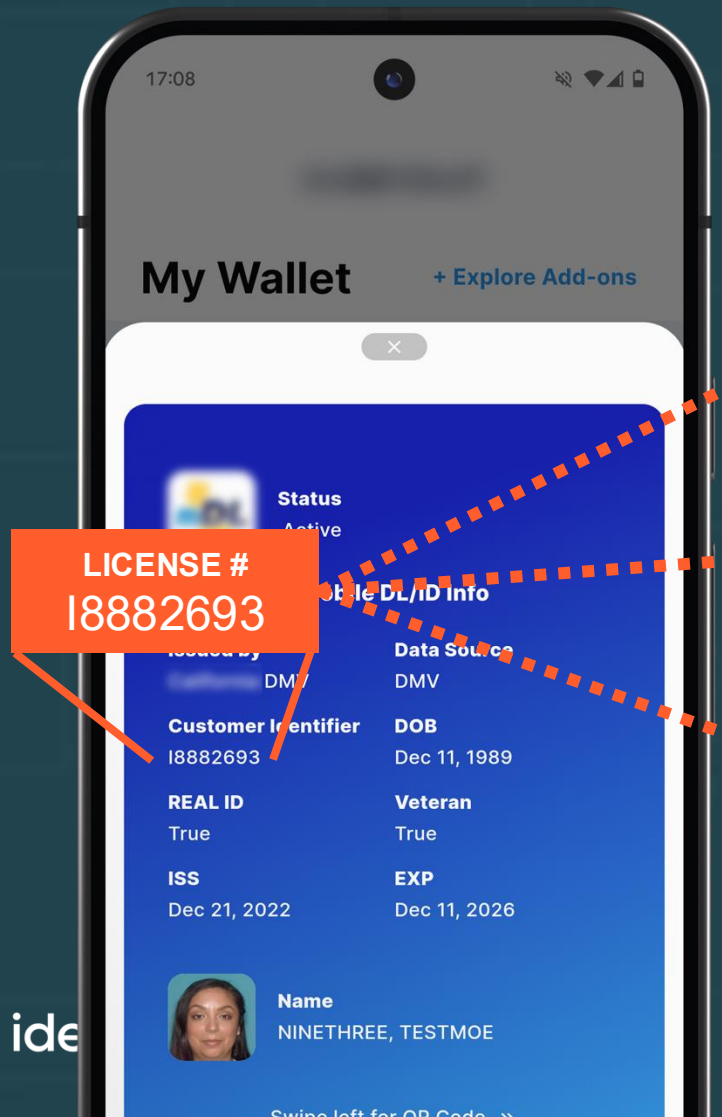
Bank — License #

COLLUSION

#identiverse

PRIVACY

VDCs as a Super Cookie



Potential Solutions

Selective Disclosure

(requires user to understand impact)

Verifier Registration & Policy/Legal

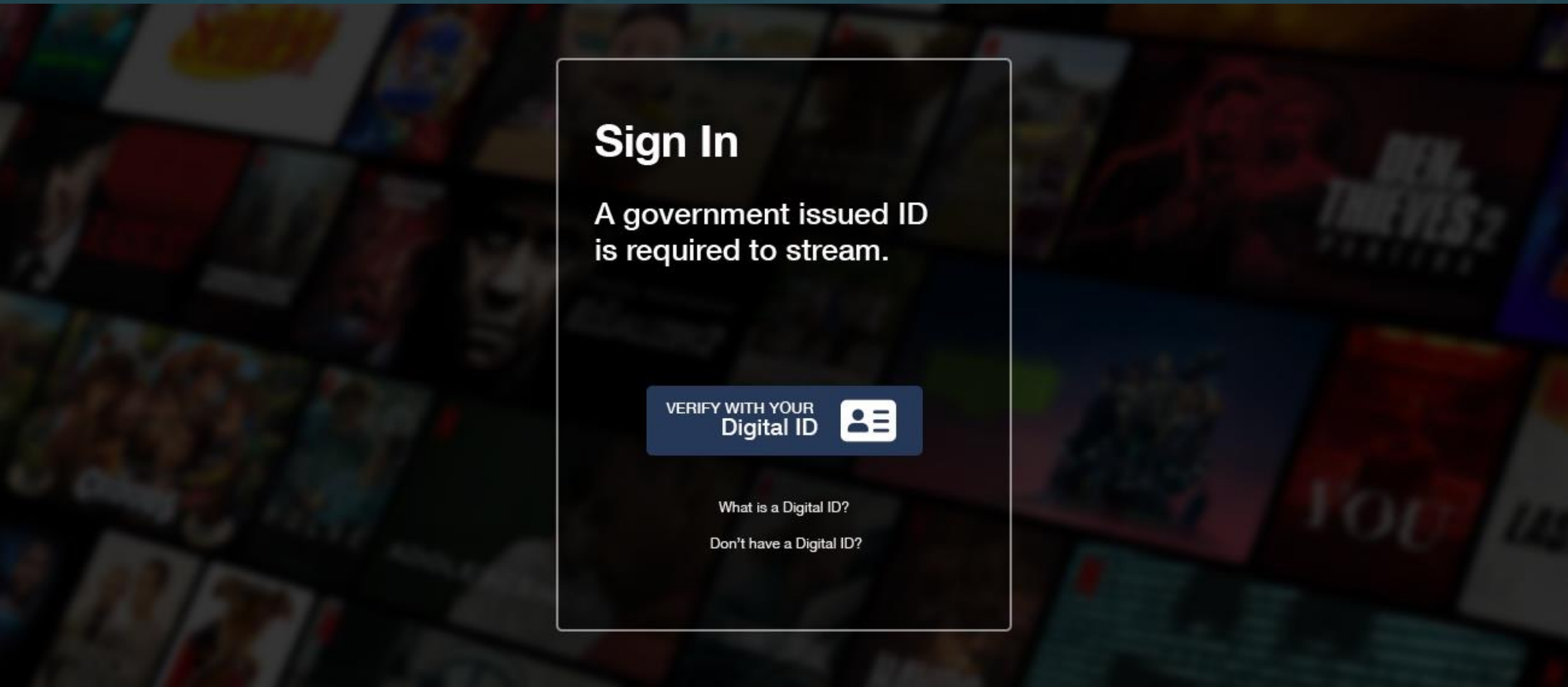
(challenging in some geos)

Zero Knowledge Proofs & Pseudonyms

(still very new)

PRIVACY

“Show Your Papers” Web



Bringing Them Together

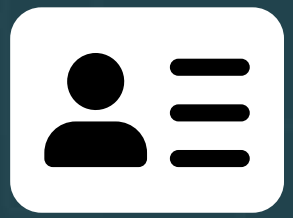
Consumer

federation -or- VDCs

sign up

passkeys

sign in



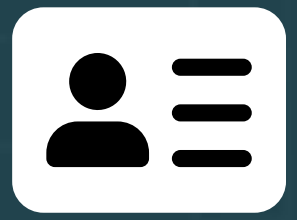
VDCs

proof up

federation -or- VDCs

recovery

Workforce (employees & contractors)



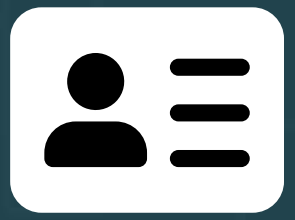
VDCs

~~**sign up**~~

onboard

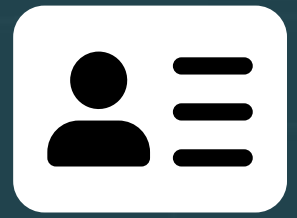
passkeys

sign in



VDCs

proof up



VDCs

recovery

Summary

- **Passkeys** for privacy preserving authentication!
- **VDCs** for user-controlled claims presentment!
- **Friends** not *foes*!

THANK YOU!

identiverse®

A CRA Resource