RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: SEM-M02

CASE STUDY: BLOCKCHAINS, IDENTITY, AND FEDERATIONS

David Chan

Cybersecurity
Ernst and Young, LLP

What we are hearing about Identity

1. A poor user experience due to multiple credentials

2. Duplicative costs for IAM infrastructure

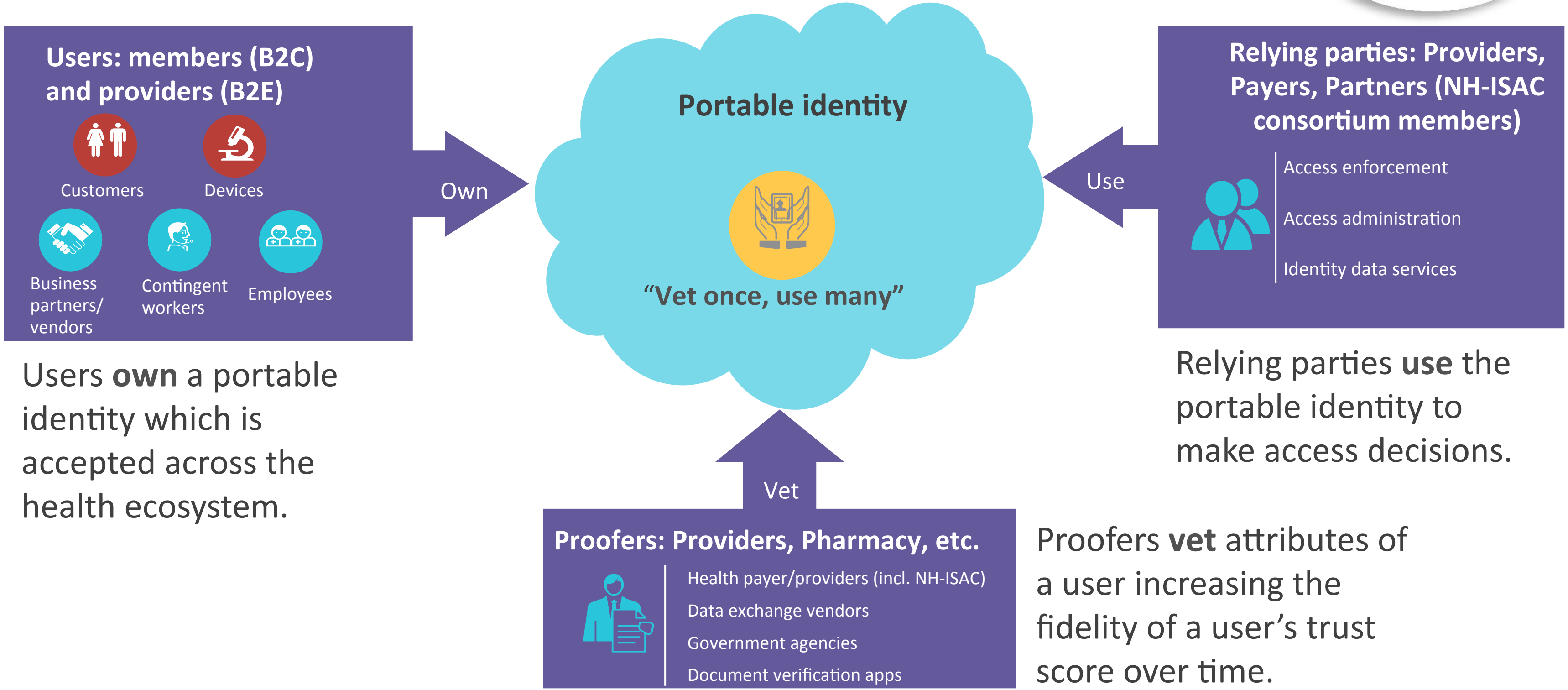
3. Expensive proofing due to dependence on for-profit entities

4. Repetitive and manual processes for provider credentialing

Leading to: Increased costs, inefficiencies, lower revenue

A DAY IN THE LIFE OF A MEMBER

Our vision: Shared identity



Users: members (B2C) and providers (B2E)

Customers

Devices

Business partners/ vendors

Contingent workers

Employees

Own

Portable identity

“Vet once, use many”

Use

Relying parties: Providers, Payers, Partners (NH-ISAC consortium members)

Access enforcement

Access administration

Identity data services

Vet

Proofers: Providers, Pharmacy, etc.

Health payer/providers (incl. NH-ISAC)

Data exchange vendors

Government agencies

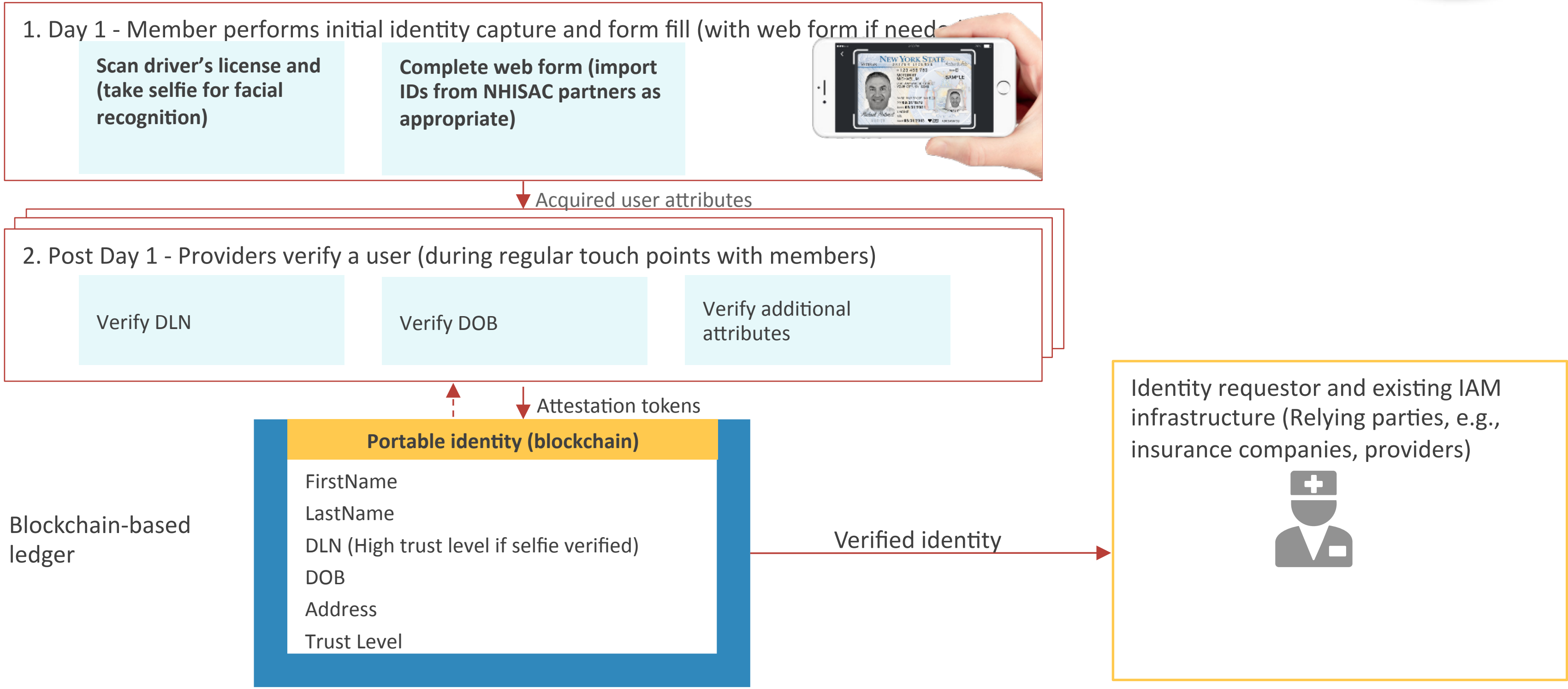
Document verification apps

Users **own** a portable identity which is accepted across the health ecosystem.

Relying parties **use** the portable identity to make access decisions.

Proofers **vet** attributes of a user increasing the fidelity of a user’s trust score over time.

Example 1: How does it work on day 1 and after?



1. Day 1 - Member performs initial identity capture and form fill (with web form if neede

Scan driver’s license and (take selfie for facial recognition)

Complete web form (import IDs from NHISAC partners as appropriate)

Acquired user attributes

2. Post Day 1 - Providers verify a user (during regular touch points with members)

Verify DLN

Verify DOB

Verify additional attributes

Attestation tokens

Portable identity (blockchain)

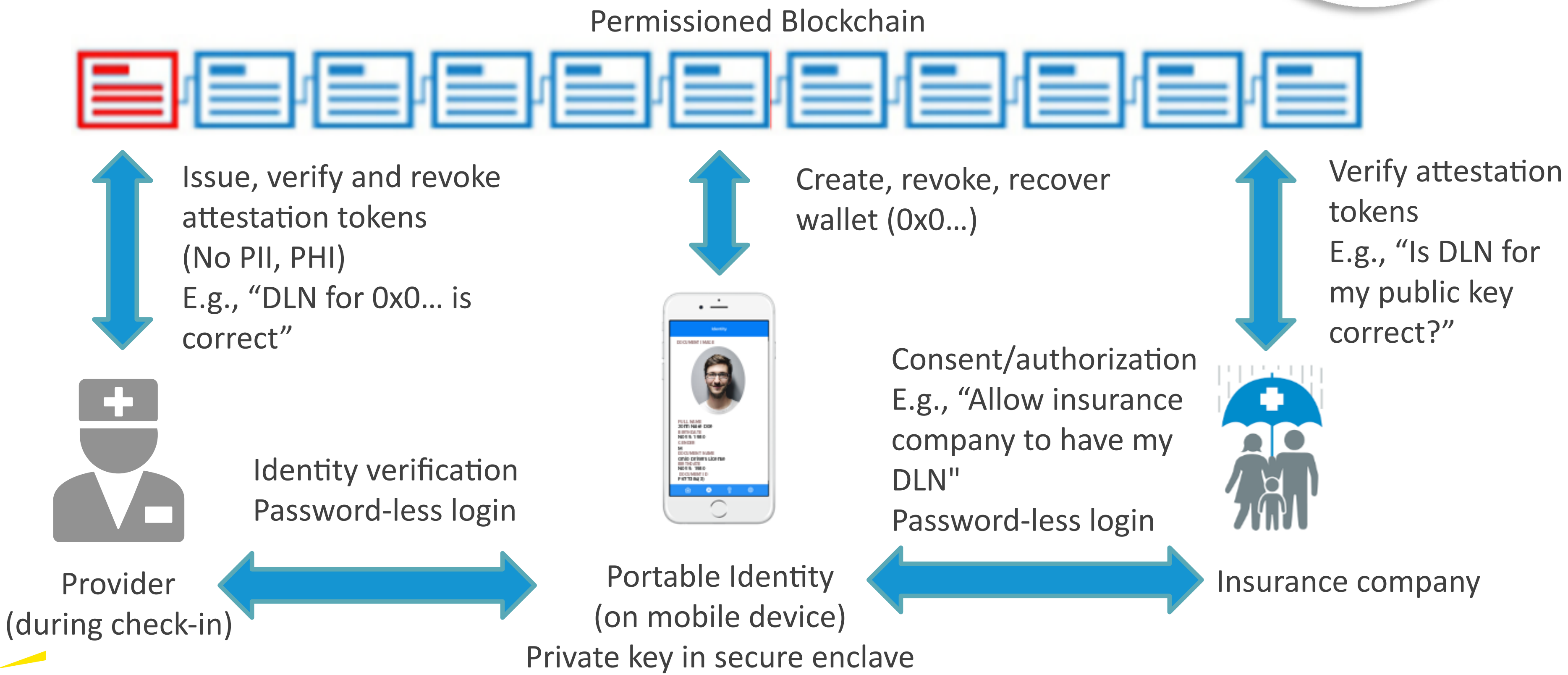
FirstName
LastName
DLN (High trust level if selfie verified)
DOB
Address
Trust Level

Blockchain-based ledger

Verified identity

Identity requestor and existing IAM infrastructure (Relying parties, e.g., insurance companies, providers)

Example 2: How does it work with blockchain?



Permissioned Blockchain

Issue, verify and revoke attestation tokens
(No PII, PHI)
E.g., “DLN for 0x0… is correct”

Create, revoke, recover wallet (0x0…)

Verify attestation tokens
E.g., “Is DLN for my public key correct?”

Identity verification
Password-less login

Consent/authorization
E.g., “Allow insurance company to have my DLN"
Password-less login

Provider
(during check-in)

Portable Identity
(on mobile device)
Private key in secure enclave

Insurance company

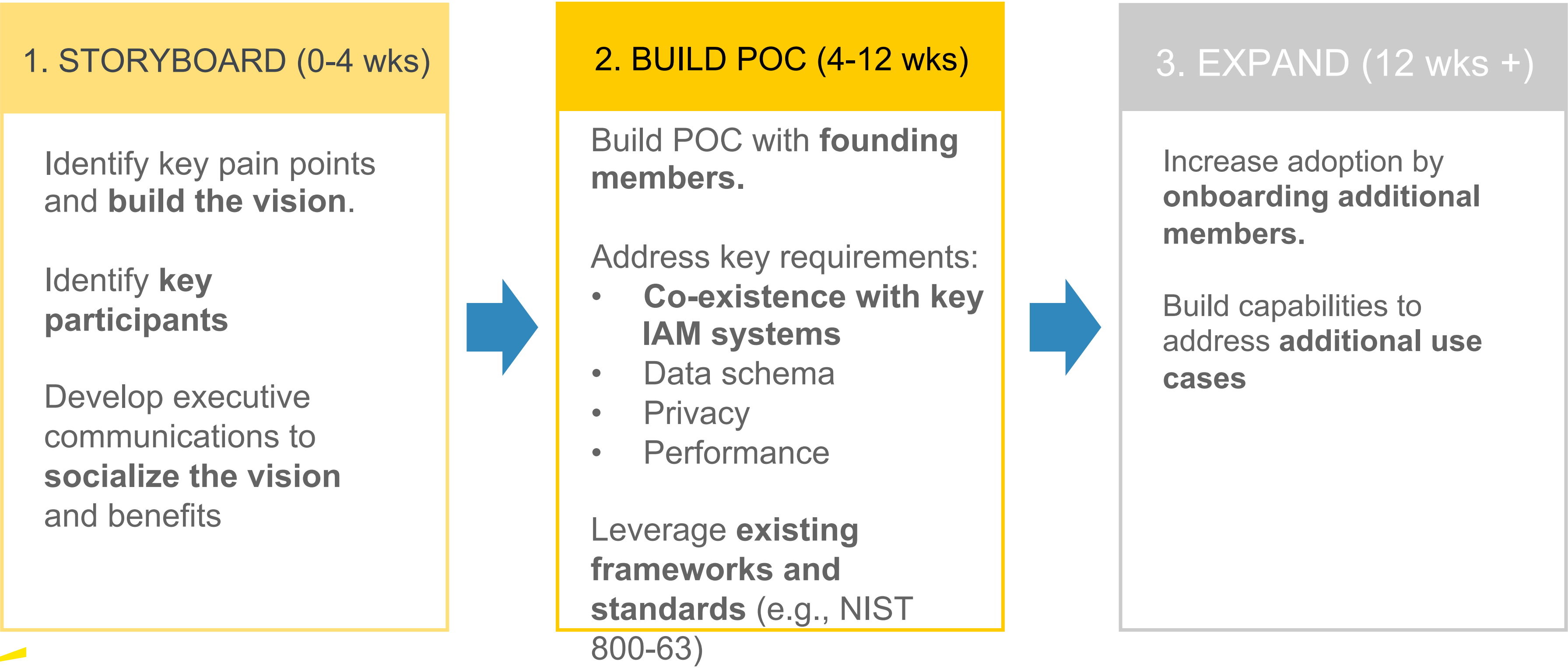
What it is NOT

- Meant to store Personal Health Information (PHI).
- A replacement for existing individual NH-ISAC consortium member IDs
- A replacement for existing IAM infrastructure (can replace certain PDP and PIP elements)
- A replacement for industry frameworks (e.g., SAFE Bio-pharma Trust Framework, NIST).
- Set in stone. We are continually incorporating feedback from the field.
- Meant to exist in a silo. Integration with other standards bodies, identity working groups is key.

How you can participate…

- Find or start **“identity working groups”** in your industry consortium, some examples:
  - Financial Services (FS-ISAC)
  - Health (NH-ISAC)
  - Telcos (Mobile Authentication Taskforce)
  - Higher Ed
  - Other industry
- Think through who your federated members would be:
  - Within your industry
  - Outside your industry (e.g., affiliates, partners)

What the effort may look like?



1. STORYBOARD (0-4 wks)

Identify key pain points and **build the vision**.

Identify **key participants**

Develop executive communications to **socialize the vision** and benefits

2. BUILD POC (4-12 wks)

Build POC with **founding members.**

Address key requirements:

- **Co-existence with key IAM systems**
- Data schema
- Privacy
- Performance

Leverage **existing frameworks and standards** (e.g., NIST 800-63)

3. EXPAND (12 wks +)

Increase adoption by **onboarding additional members.**

Build capabilities to address **additional use cases**

THANK YOU - Q&A

For a deeper dive, come to:
“Can Blockchain Enable Identity Management?”
April 19, 2018 1:45 PM - 2:30 PM

APPENDIX - TECHNICAL DEMO

Day 1 - Member Enrollment

On Day 1 - Enrollment

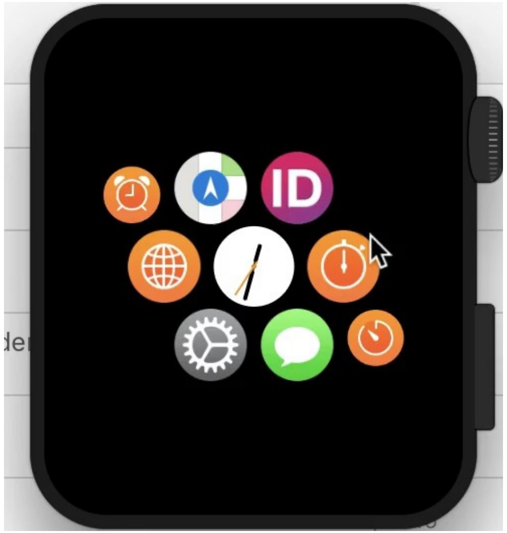
- Seamless enrollment on Day 1 by:
  - Importing existing IDs with NH-ISAC partners
  - Form fill thru driver’s license scan
- Trust Level 1 verification with self asserted attributes
- Trust Level 2 with remote driver’s license verification

Going to the provider

When going to the provider

- “Passwordless” login through biometrics (e.g., FaceID)
- Easy check-in at provider’s office by QR code scan
- Similar to a mobile boarding pass

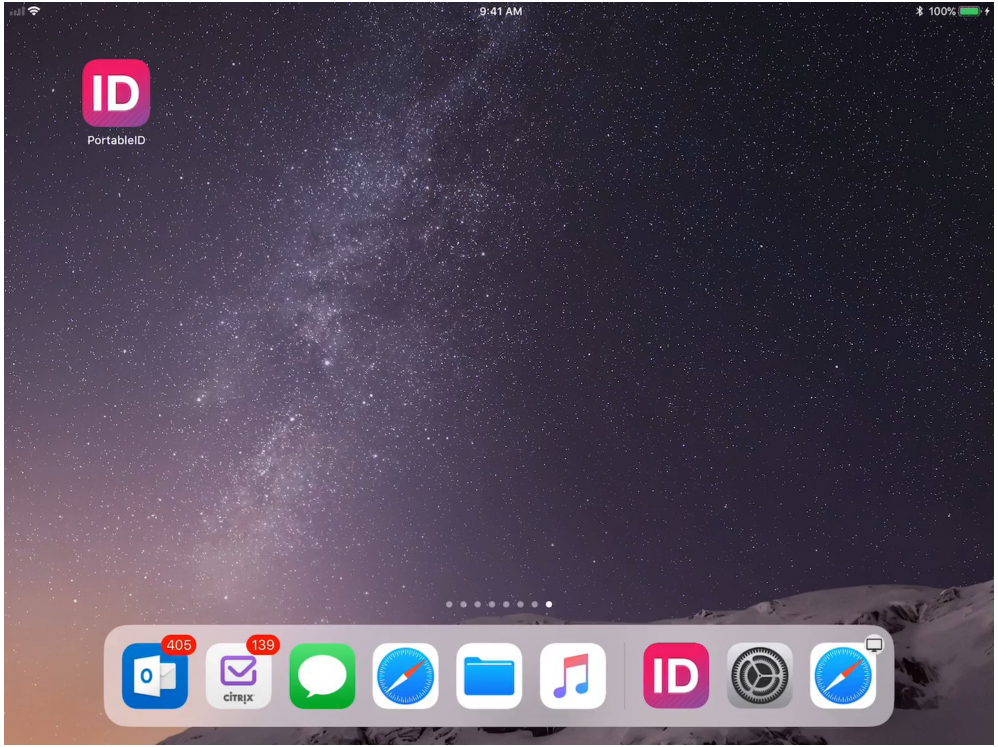
Wearable check-in – for those with their hands full…



- Added convenience without having to reach for your phone

Checking the member in

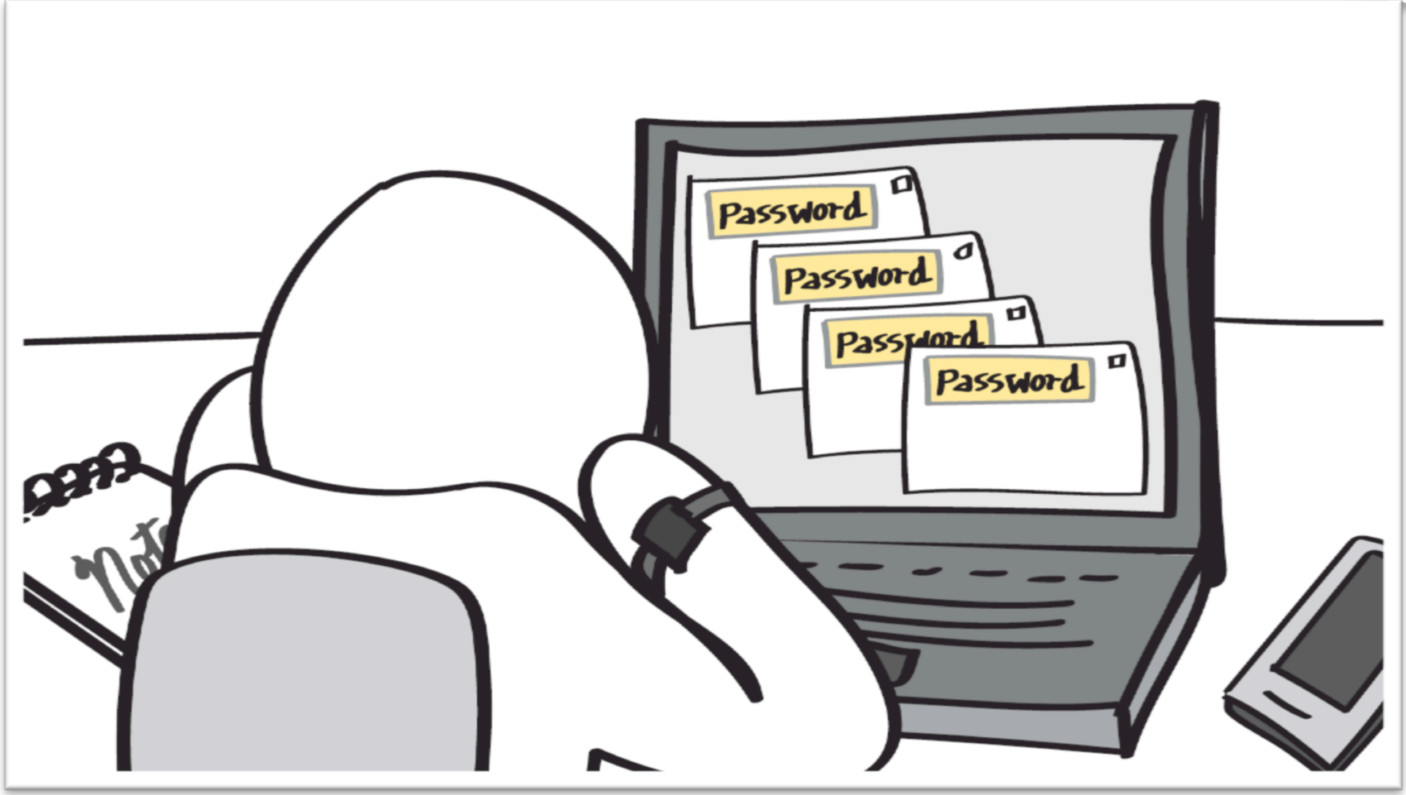
Provider's perspective – what the receptionist at the provider does...



- Provider has a companion app in the office
- On an iPad
- Provider verifies the ID concurrently with check-in
- Trust Level 3 – in-person verification with provider
- Usage / assertion history can be used by insurance provider for proofing (optional)

Stills from “Day in the life video”

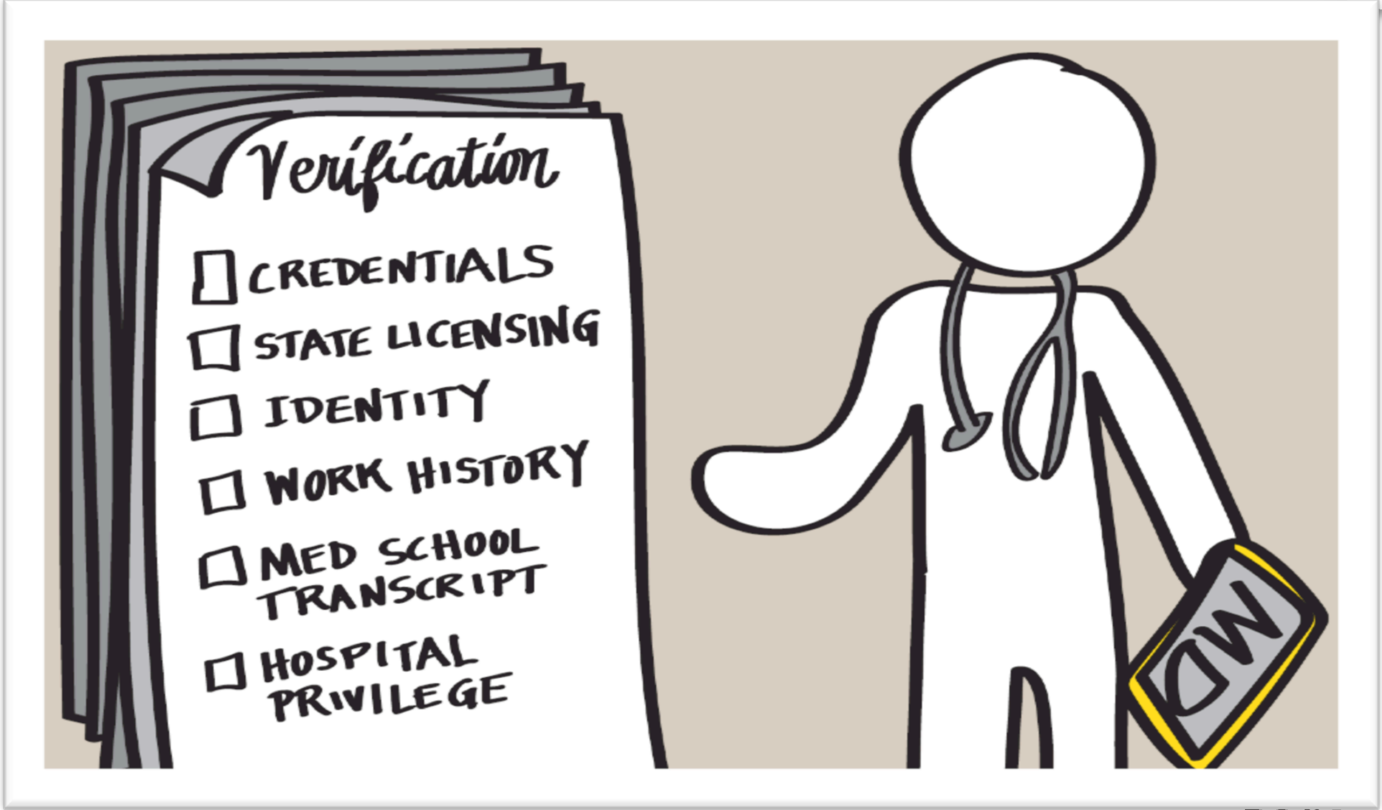
Poor digital experience



Duplicative costs and expensive proofing

Application ⇒ ASK
? medical history
? employment history
? attributes - other
GET INSURANCE
PENDING APPLICATIONS

Repetitive verification processes


Verification
□ CREDENTIALS
□ STATE LICENSING
□ IDENTITY
□ WORK HISTORY
□ MED SCHOOL TRANSCRIPT
□ HOSPITAL PRIVILEGE
MD