KeyShare

by PassiveBolt™

SSI based Access Control

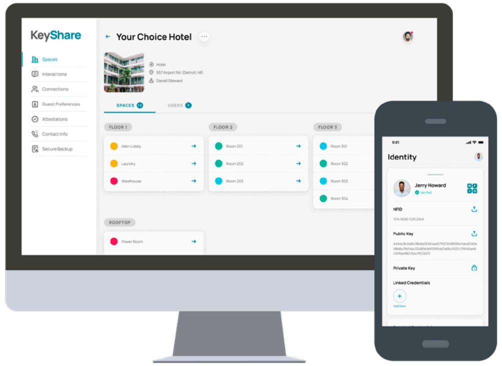
Personal Data Store

P2P Interactions

Attestations

Decentralised Identifier

Workflows



HFTP presents HITEC® — 2023 Innovation Award

CES Innovation Awards 2021 Honoree

CES Innovation Awards 2020 Honoree

Forbes NEXT 1000 Honoree 2021

3 Granted & 2 Pending Patents

Forbes — Top 7 Unmissable Tech 2020

Internet of Things World Nominee — Best 2020 Consumer IoT

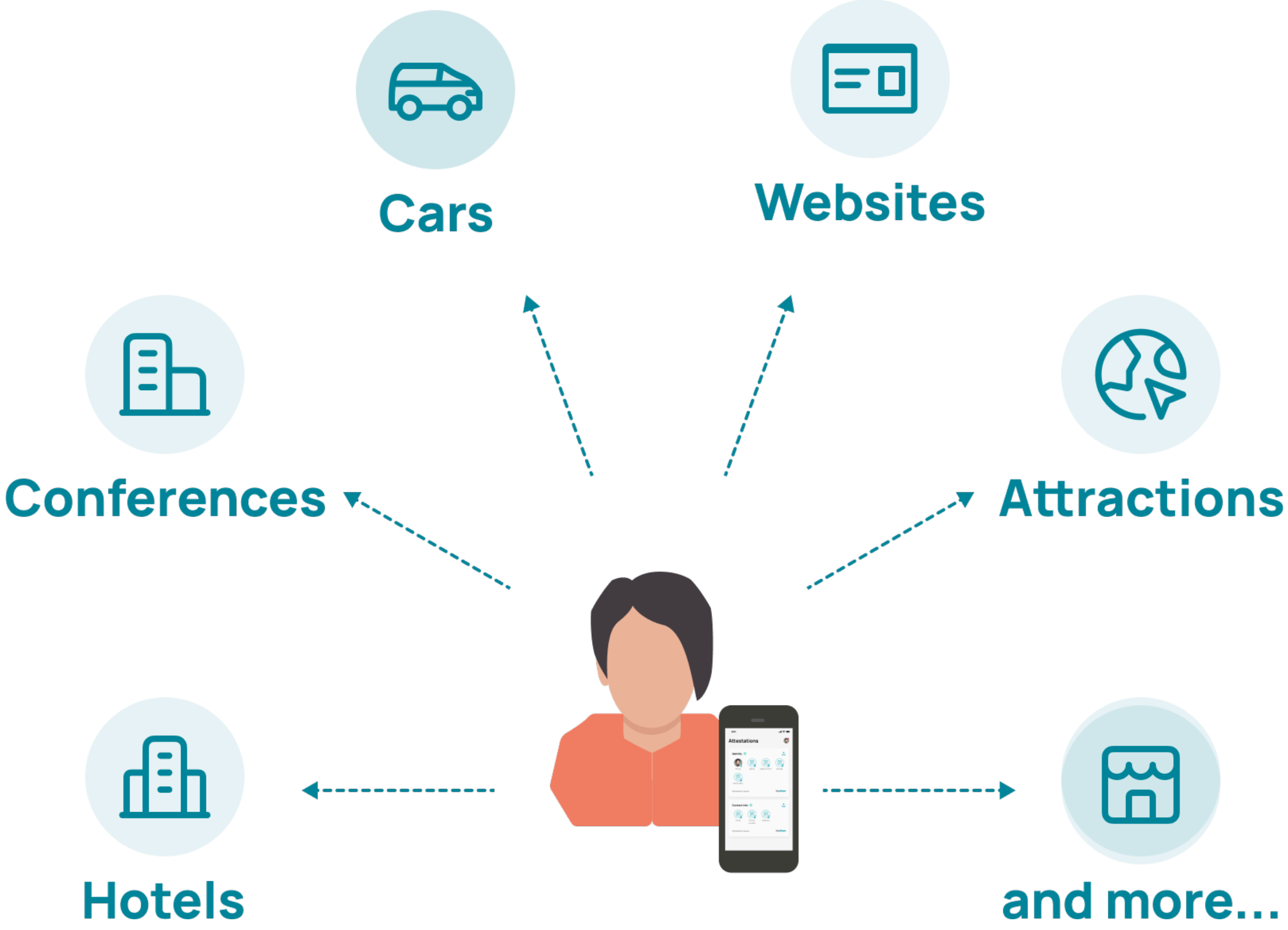
Overview

- Background and Concept
- Key Components of SSI
- Example Use Cases
- Intro to KeyShare

Background and Concepts

Concept

Identity



Cars

Websites

Conferences

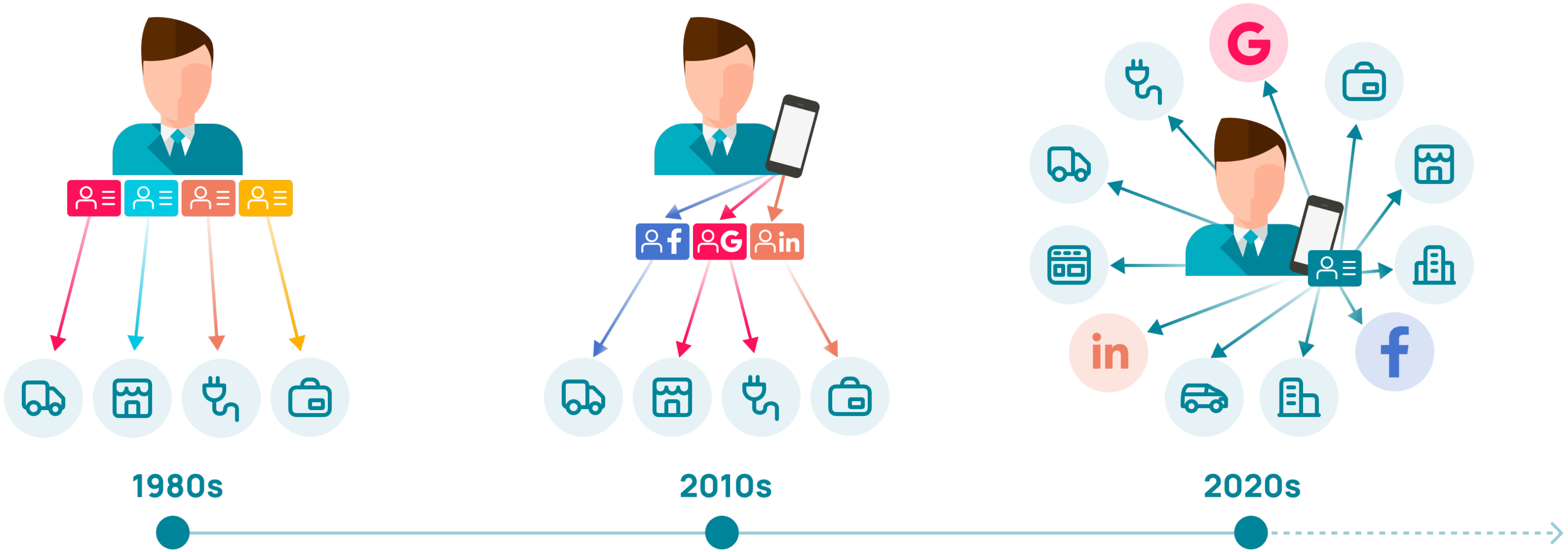
Attractions

Hotels

and more…

Intro to SSI

What is Self-sovereign identity (SSI)?



Centralized Identity

- ✗ Security
- ✗ Privacy
- ✗ User Experience

Federated Identity

- ✗ Security
- ✗ Privacy
- ✓ User Experience

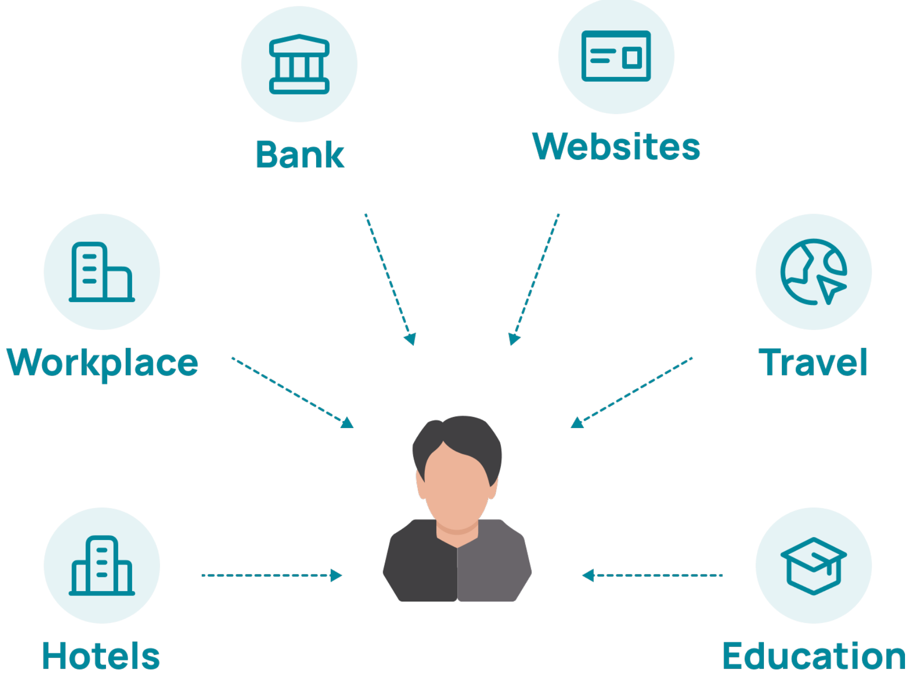
Self-Sovereign Identity

- ✓ Security
- ✓ Privacy
- ✓ User Experience

W3C® DIF TRUST Over IP FOUNDATION

Principles of SSI

- **Control**: Users have authority over their own identity
- **Access**: Users decide who can access their data
- **Transparency**: Clear policies on data usage
- **Portability**: Ability to use identity across different platforms



Key Components of SSI

Key Components of SSI

Decentralized Identifier (DIDs)

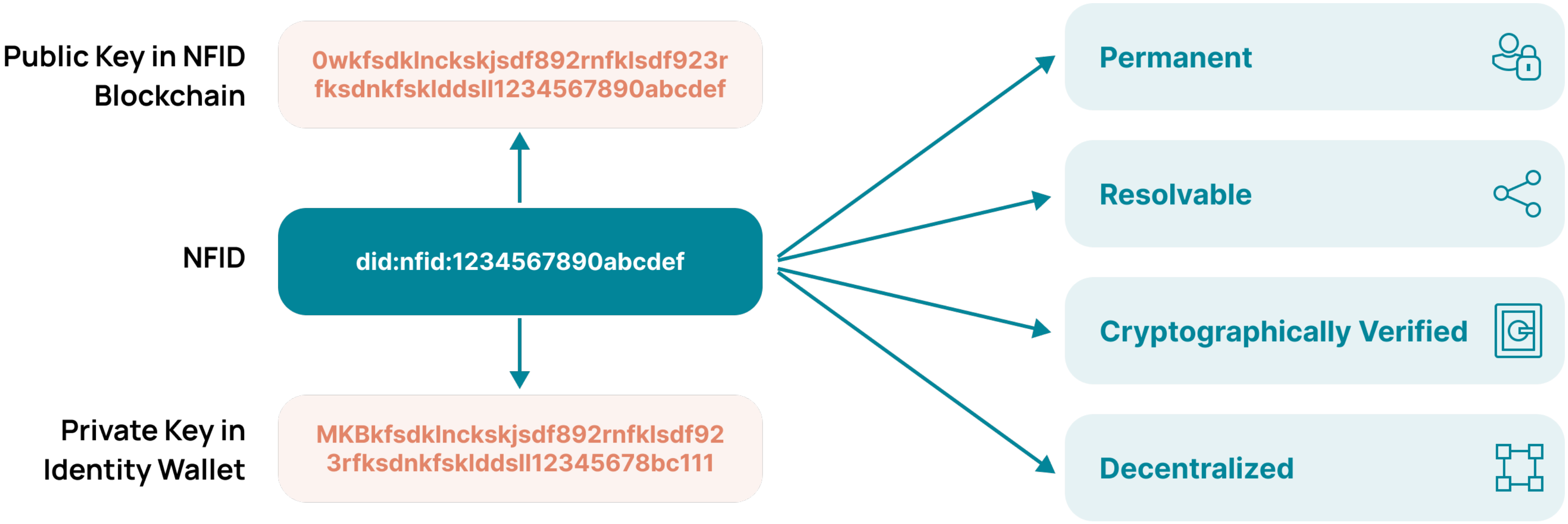
Decentralized Identifiers (DIDs) are globally unique, persistent, and resolvable identifiers that enable individuals, organizations, and things to establish and control their digital identity.

did:nfid:1234567890abcdef

A Decentralized Identifier, or DID, is a URI composed of three parts: the scheme did:, a method identifier, and a unique, method-specific identifier specified by the DID method.

Key Components of SSI

Decentralized Identifier (DIDs)



Public Key in NFID Blockchain

0wkfsdklnckskjsdf892rnfklsdf923r fksdnkfsklddsll1234567890abcdef

NFID

did:nfid:1234567890abcdef

Private Key in Identity Wallet

MKBkfsdklnckskjsdf892rnfklsdf92 3rfksdnkfsklddsll12345678bc111

Permanent

Resolvable

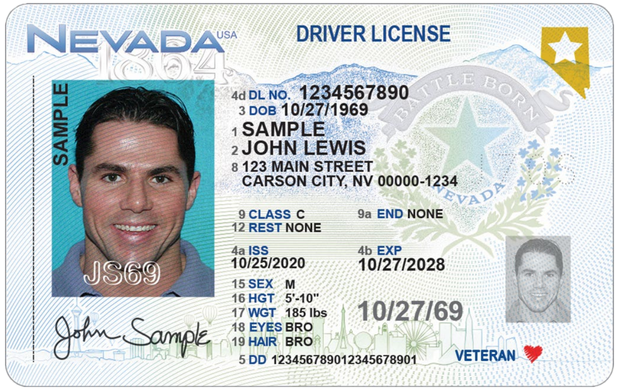
Cryptographically Verified

Decentralized

Standards Body: W3C

Attestation (VC) Example

A verifiable credential is a digitally signed attestation of a fact or claim about an entity, such as a person's identity, qualifications, or attributes, that can be cryptographically verified by others.



NEVADA USA DRIVER LICENSE

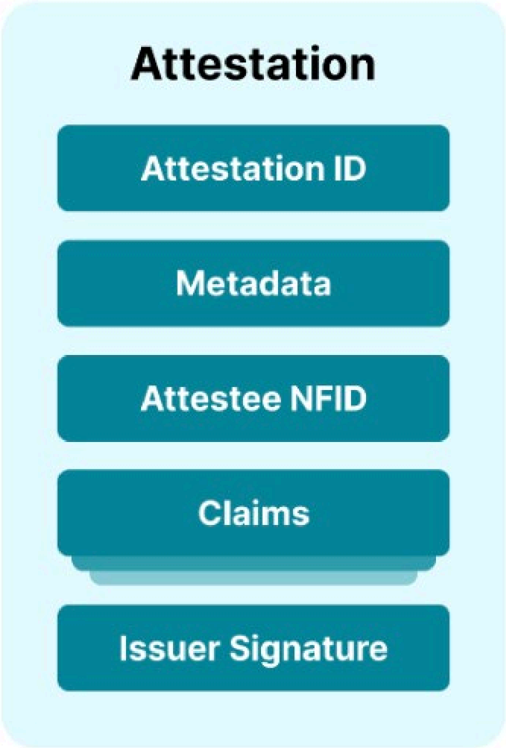
SAMPLE

4d DL NO. 1234567890
3 DOB 10/27/1969
1 SAMPLE
2 JOHN LEWIS
8 123 MAIN STREET
CARSON CITY, NV 00000-1234

9 CLASS C
9a END NONE
12 REST NONE
4a ISS 10/25/2020
4b EXP 10/27/2028
15 SEX M
16 HGT 5'-10"
17 WGT 185 lbs
18 EYES BRO
19 HAIR BRO
10/27/69
5 DD 123456789012345678901
VETERAN

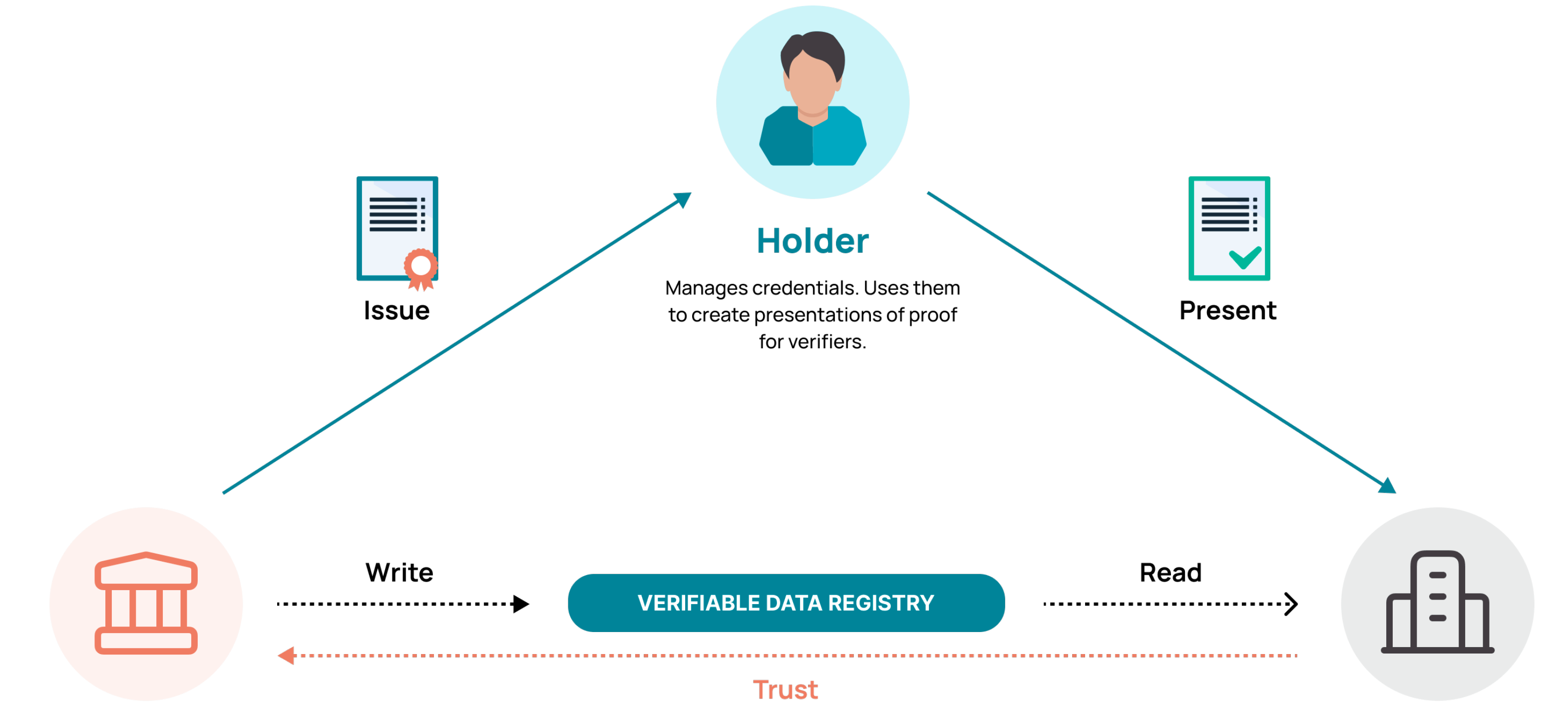
John Sample

1864
JS69
BATTLE BORN
NEVADA



Key Components of SSI

Trust Triangle



Manages credentials. Uses them to create presentations of proof for verifiers.

Issuer

Digitally signs attestations and issues it to the holder.

Verifier

Requests proof. Verifies the validity of the attestation.

Example Use Cases

Use Cases

Access Control

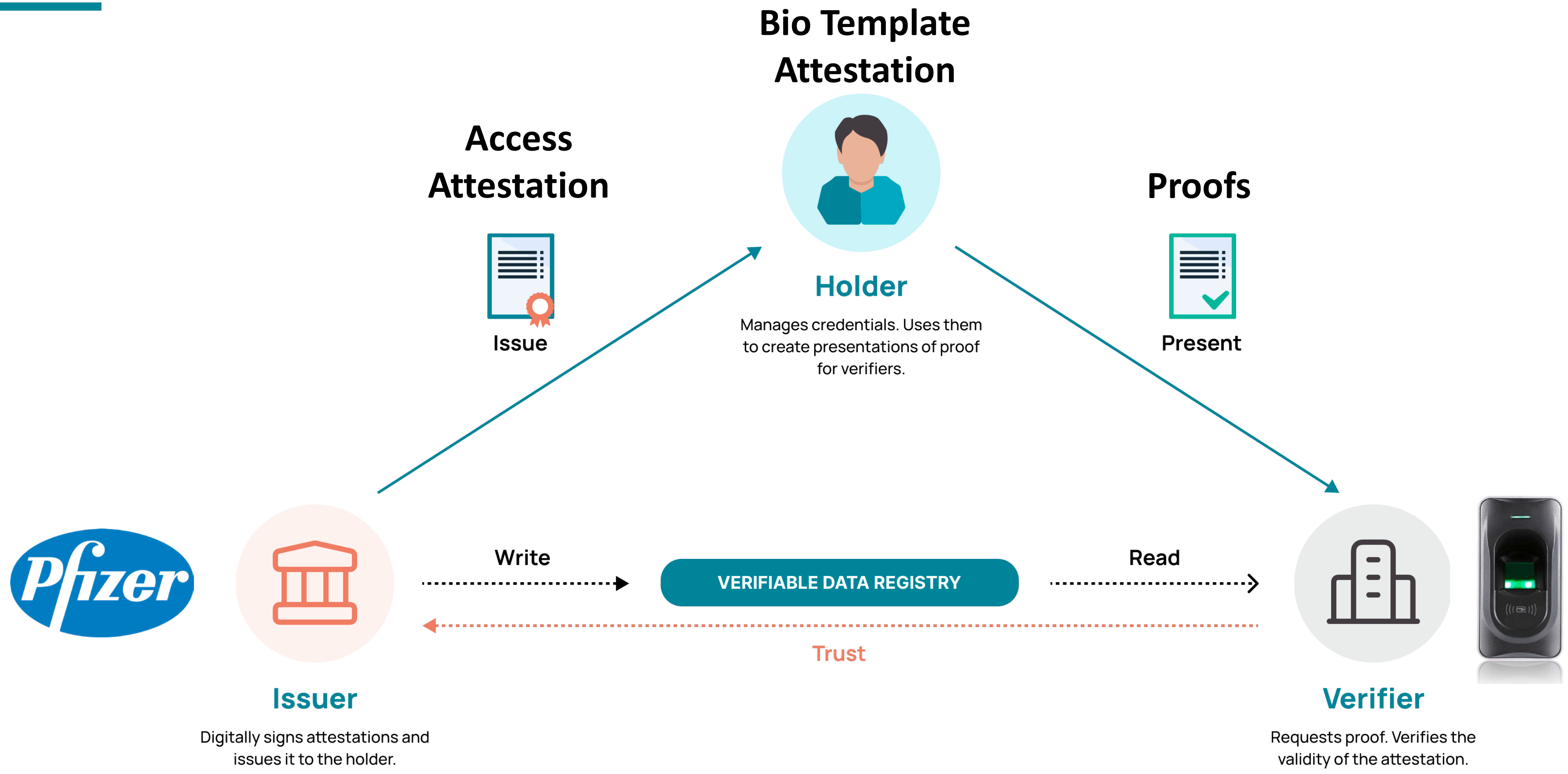
SSI as an enabler for secure, decentralized access control

- Reimagining access control with SSI
- Trust without centralized authorities

Some advantages over traditional access control systems

- Improved security: Decentralized systems reduce breach risks
- User-centric: Empowering users to manage access
- Enhanced privacy: Minimizing unnecessary data storage
- Compliance by design to expanding privacy laws (GDPR, BIPA, CCPA, VCPA, CO, NY etc.)

Decentralized Biometrics



Bio Template Attestation

Holder

Manages credentials. Uses them to create presentations of proof for verifiers.

Access Attestation

Issue

Proofs

Present

Issuer

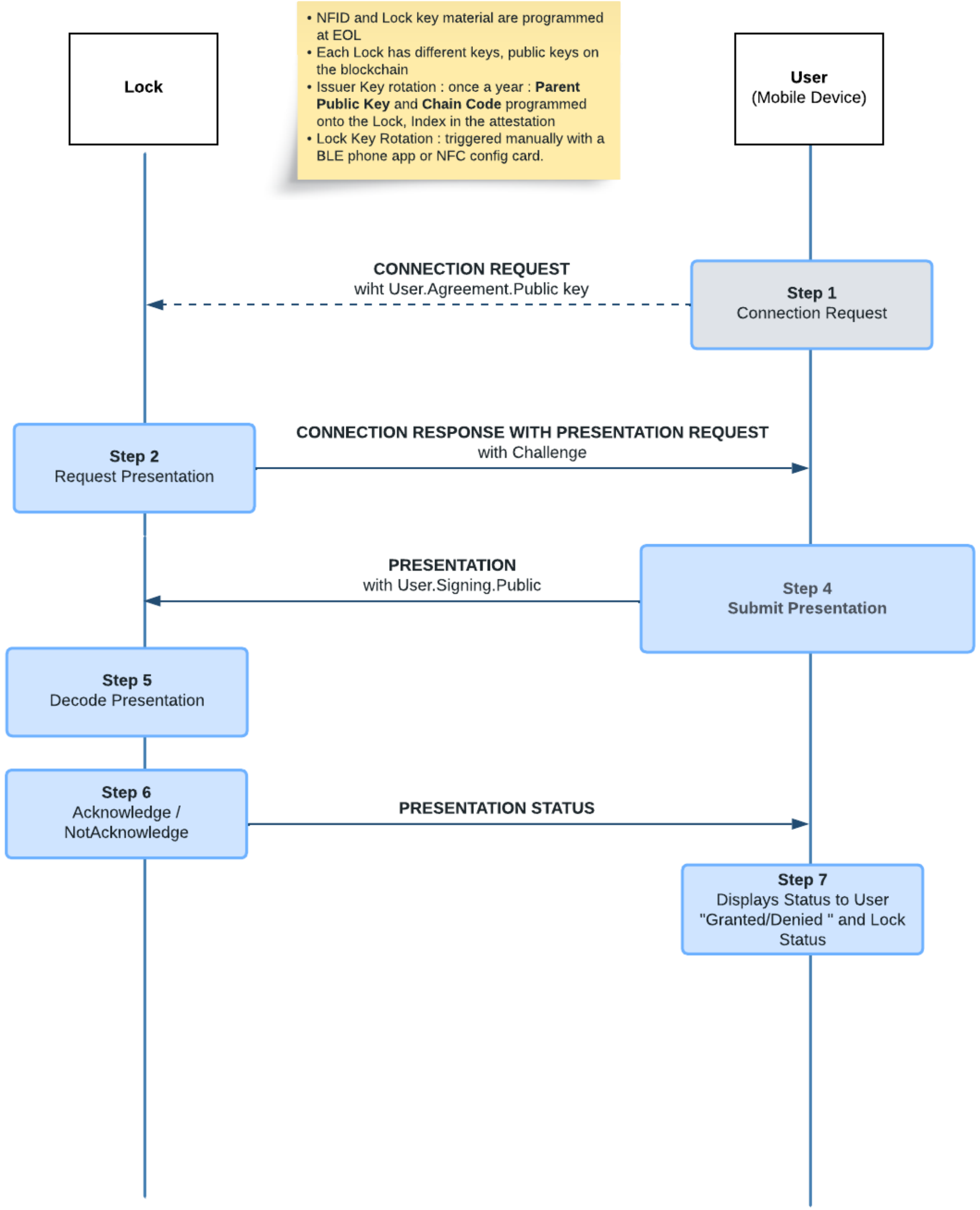
Digitally signs attestations and issues it to the holder.

Verifier

Requests proof. Verifies the validity of the attestation.

Use Cases

BLE Communication Flow



Lock

User
(Mobile Device)

- NFID and Lock key material are programmed at EOL
- Each Lock has different keys, public keys on the blockchain
- Issuer Key rotation : once a year : **Parent Public Key** and **Chain Code** programmed onto the Lock, Index in the attestation
- Lock Key Rotation : triggered manually with a BLE phone app or NFC config card.

Step 1
Connection Request

CONNECTION REQUEST
wiht User.Agreement.Public key

Step 2
Request Presentation

CONNECTION RESPONSE WITH PRESENTATION REQUEST
with Challenge

Step 4
Submit Presentation

PRESENTATION
with User.Signing.Public

Step 5
Decode Presentation

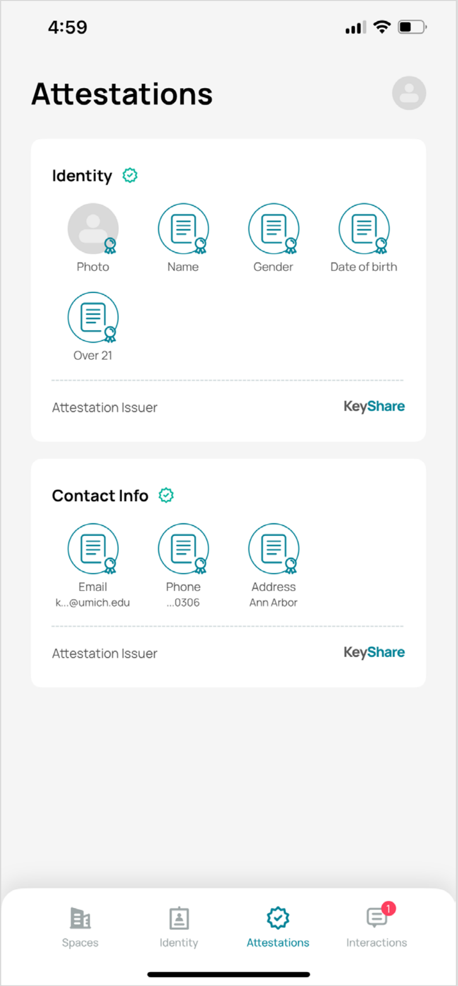
Step 6
Acknowledge /
NotAcknowledge

PRESENTATION STATUS

Step 7
Displays Status to User
"Granted/Denied " and Lock
Status

Intro to KeyShare

Intro to KeyShare



4:59

Attestations

Identity

Photo · Name · Gender · Date of birth · Over 21

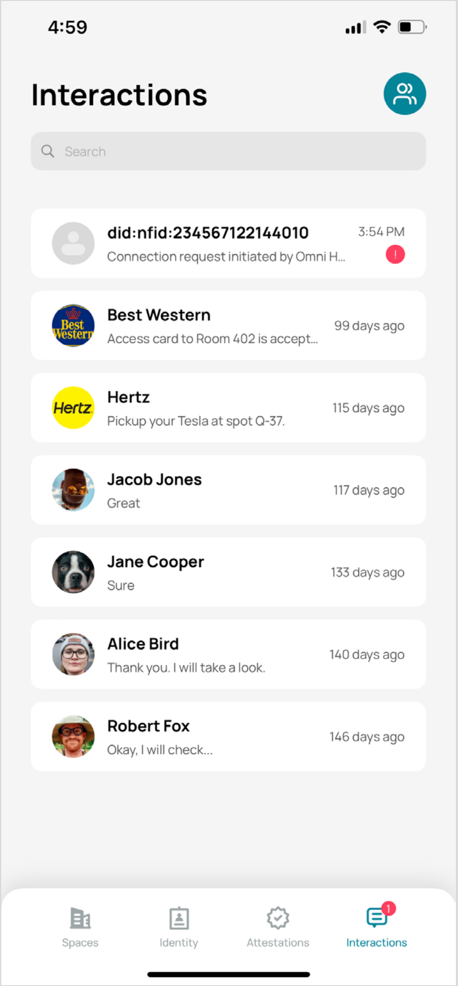
Attestation Issuer — KeyShare

Contact Info

Email k...@umich.edu · Phone ...0306 · Address Ann Arbor

Attestation Issuer — KeyShare

Securely store & share traveler profile



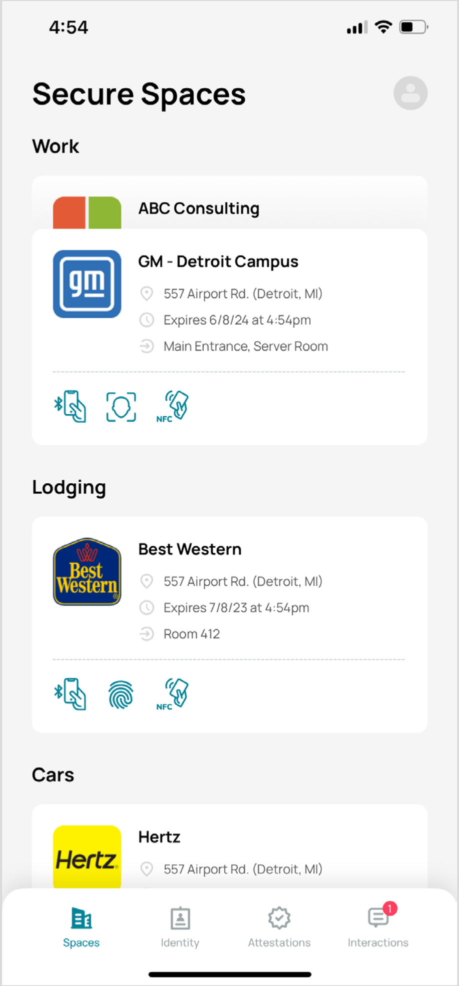
4:59

Interactions

Search

did:nfid:234567122144010	Connection request initiated by Omni H...	3:54 PM
Best Western	Access card to Room 402 is accept...	99 days ago
Hertz	Pickup your Tesla at spot Q-37.	115 days ago
Jacob Jones	Great	117 days ago
Jane Cooper	Sure	133 days ago
Alice Bird	Thank you. I will take a look.	140 days ago
Robert Fox	Okay, I will check...	146 days ago

Interact with traveler providers



4:54

Secure Spaces

Work

ABC Consulting

GM - Detroit Campus
557 Airport Rd. (Detroit, MI)
Expires 6/8/24 at 4:54pm
Main Entrance, Server Room

Lodging

Best Western
557 Airport Rd. (Detroit, MI)
Expires 7/8/23 at 4:54pm
Room 412

Cars

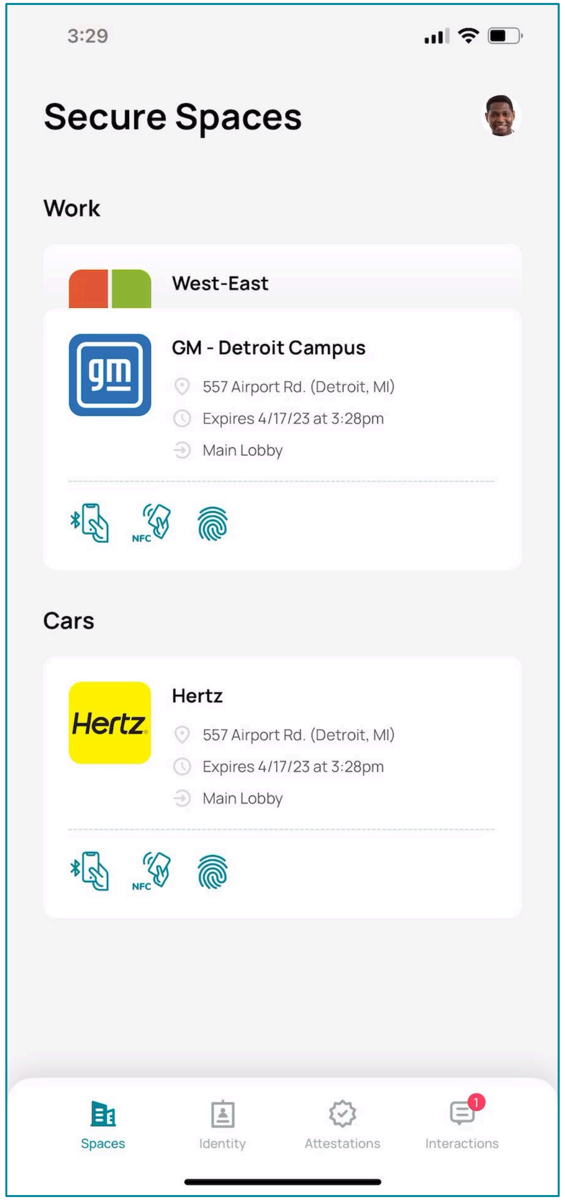
Hertz
557 Airport Rd. (Detroit, MI)

Receive access (e.g. keys, pass)

PassiveBolt

Intro to KeyShare

KeyShare Wallet



Secure Spaces

Work

West-East

GM - Detroit Campus

557 Airport Rd. (Detroit, MI)

Expires 4/17/23 at 3:28pm

Main Lobby

Cars

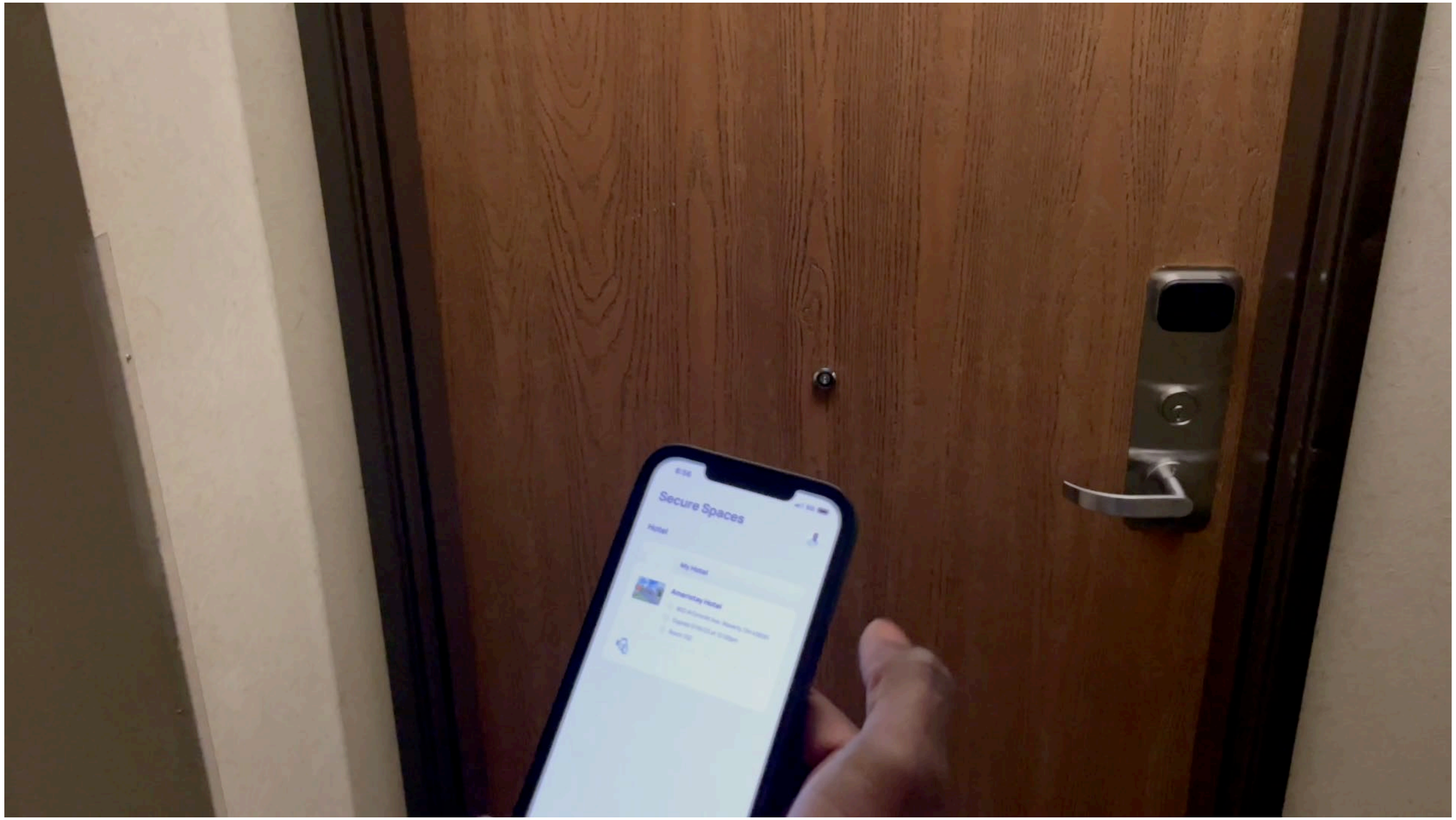
Hertz

557 Airport Rd. (Detroit, MI)

Expires 4/17/23 at 3:28pm

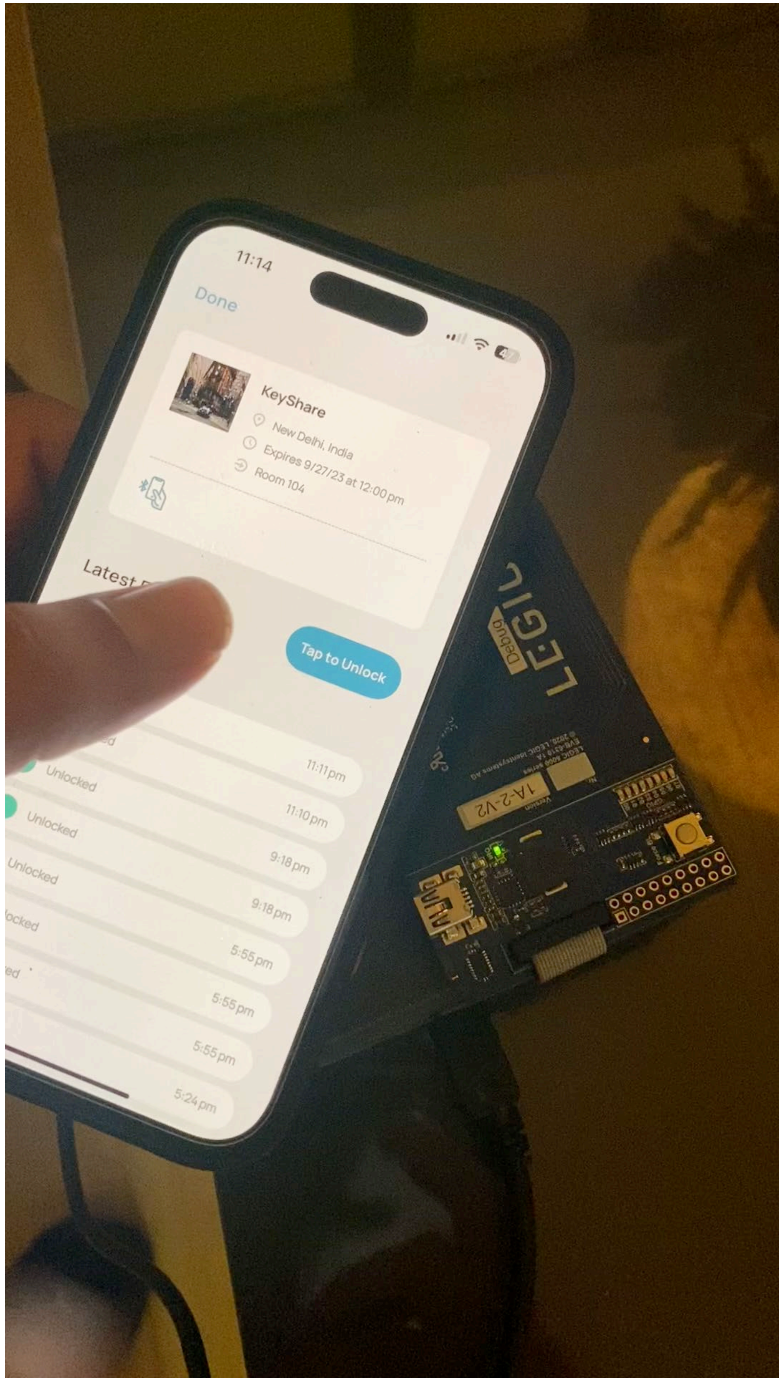
Main Lobby

Mobile Key



Intro to KeyShare

Mobile Key (Legic)

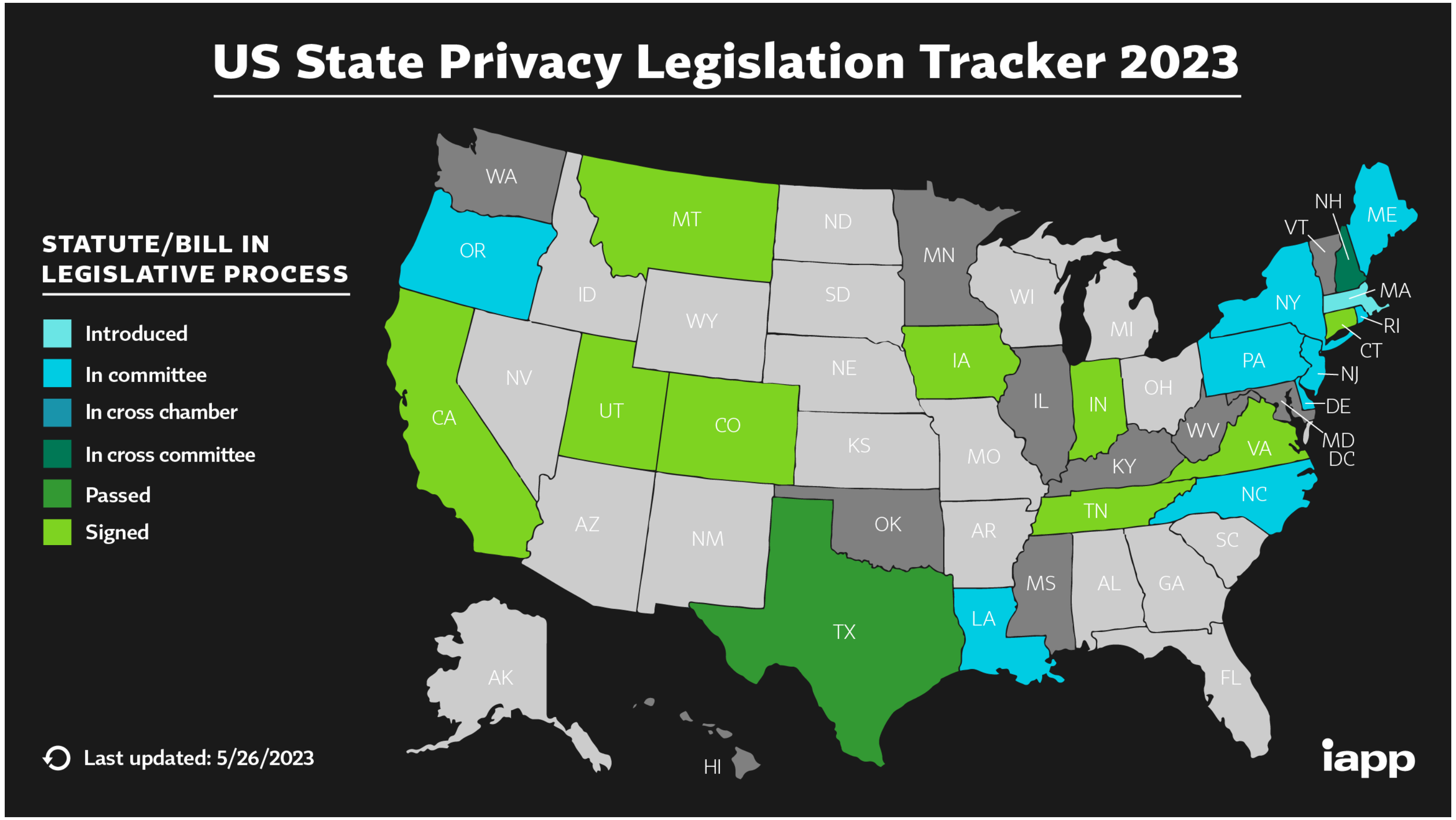


PassiveBolt

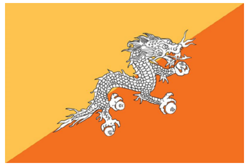
Future Trends and Developments

Adoption of SSI

SSI has significant legislative momentum



eIDAS



Bhutan National ID

Adoption of SSI

...along with institutional and industry momentum

UNITED NATIONS

U.S. DEPARTMENT OF HOMELAND SECURITY

Canada

European Commission

U.S. Customs and Border Protection

Massachusetts Institute of Technology

GS1

Microsoft

intel

and many more...

Standards Development

Future Trends and Development

- Governance and Trust Framework

TRUST Over IP FOUNDATION

eIDAS

- New standards and protocols: Evolving the SSI ecosystem

NFID Foundation

DIF

OpenWallet FOUNDATION

Thank you

We invite you to join us on this exciting journey into the future of access control by empowering users to control their digital identities and access both digital and physical spaces without compromising privacy or identity data.

Contact

Name: Simon Forster | **Email**: simon@passivebolt.com | **Phone**: +49 (171) 5033142