Verifiable Credentials 101 for SSI

An intro and technical explanation

September 18, 2018

Tyler Ruff

Product Manager, Evernym

SSIMeetup.org

SSIMeetup objectives

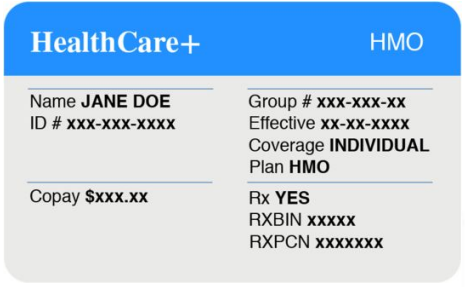
1. Empower global SSI communities
2. Open to everyone interested in SSI
3. All content is shared with CC BY SA

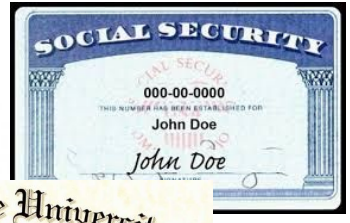
Alex Preukschat @SSIMeetup @AlexPreukschat
Coordinating Node SSIMeetup.org

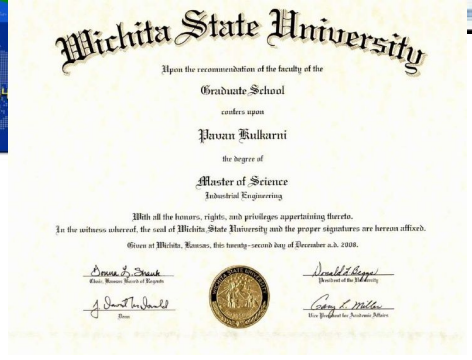
What is a Credential?

Today, usually just “proof” of something about ourselves

Most credentials are physical







Problems with today's credentials

- Easy to fake / forge
- Easy to impersonate the true owner
- Can be lost or damaged
- Expensive to create and issue
- Can't scale
- Can't be easily verified online
- Disclose more than is needed

What are Verifiable Credentials?

A digital attestation of one Identity Owner about another

Also called Attestations or Claims

What is an Identity Owner?

A person or organization which has digital control over it’s things

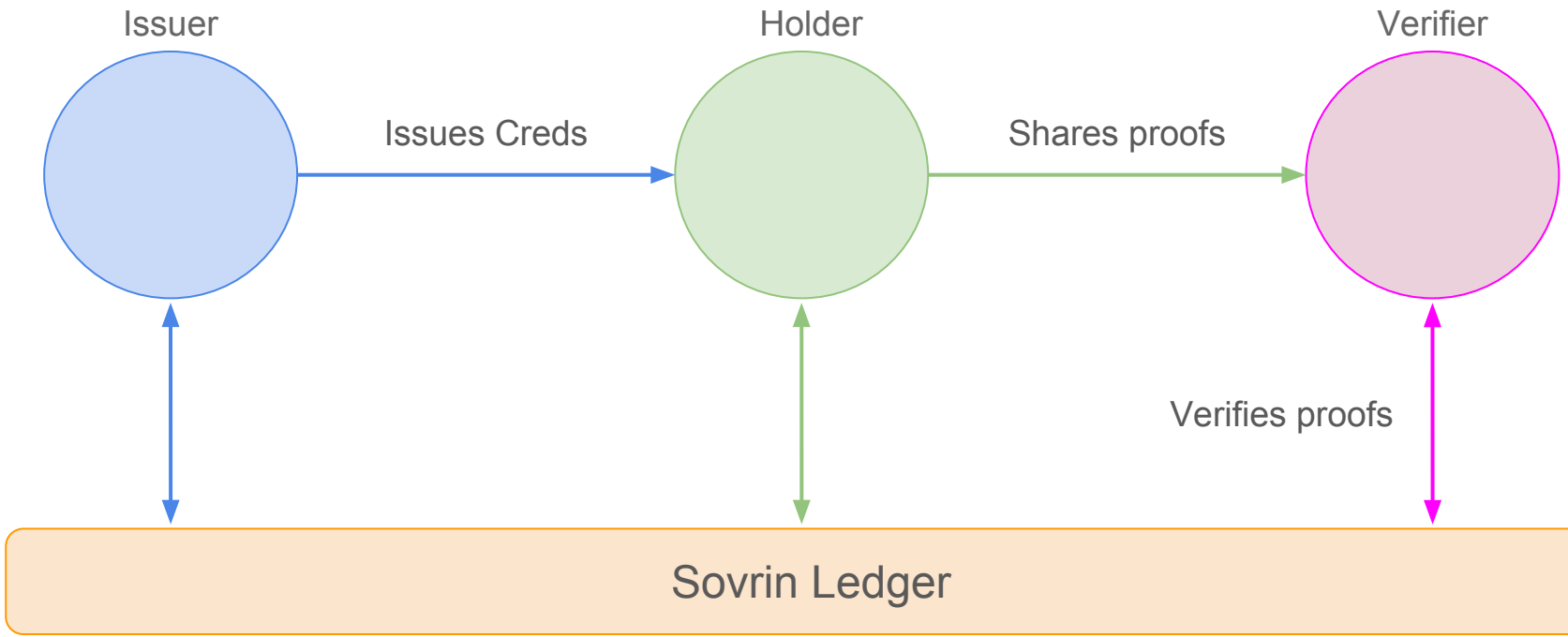
Verifiable Credentials are:

- All digital, under the true owner's control
- High scalability
- Much harder to fake
- Much harder to impersonate true owner
- Eliminates need for treasure troves of data
- Enables minimum disclosure
- Enables Zero-Knowledge Proofs
- Data by itself becomes useless to thieves

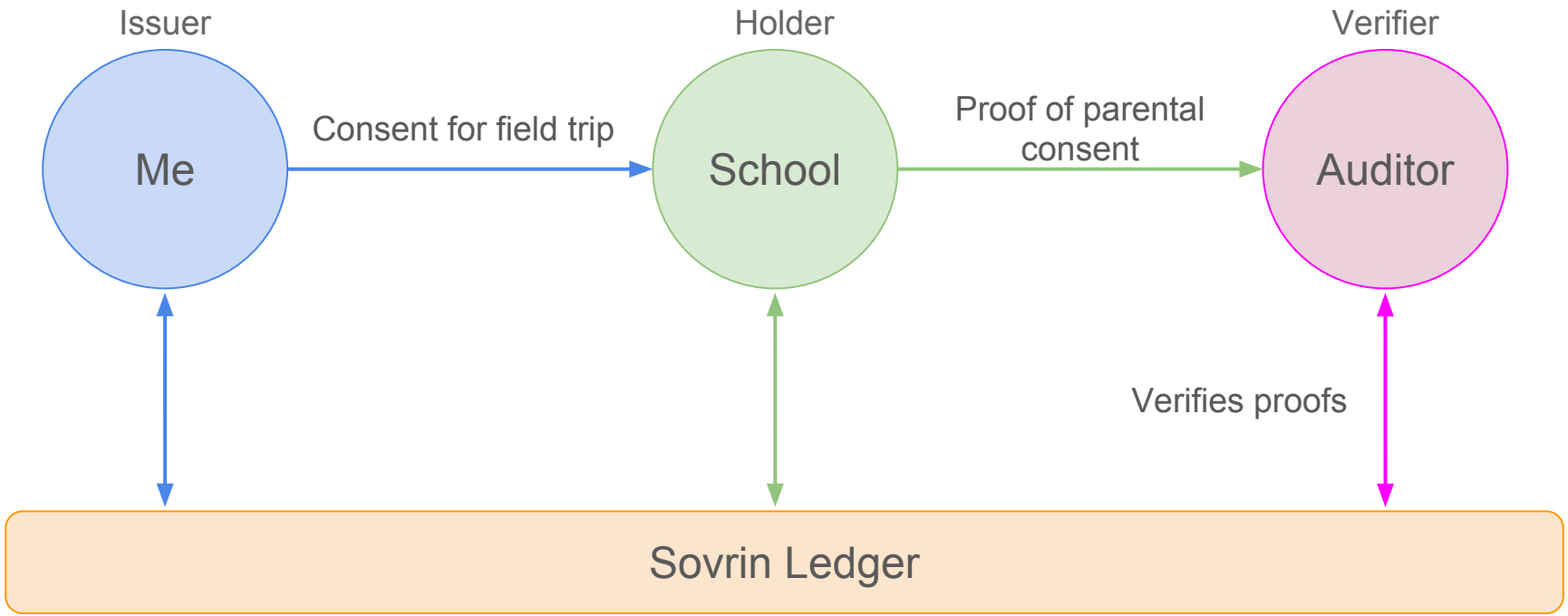
How do you get a Verifiable Credential?

Three roles

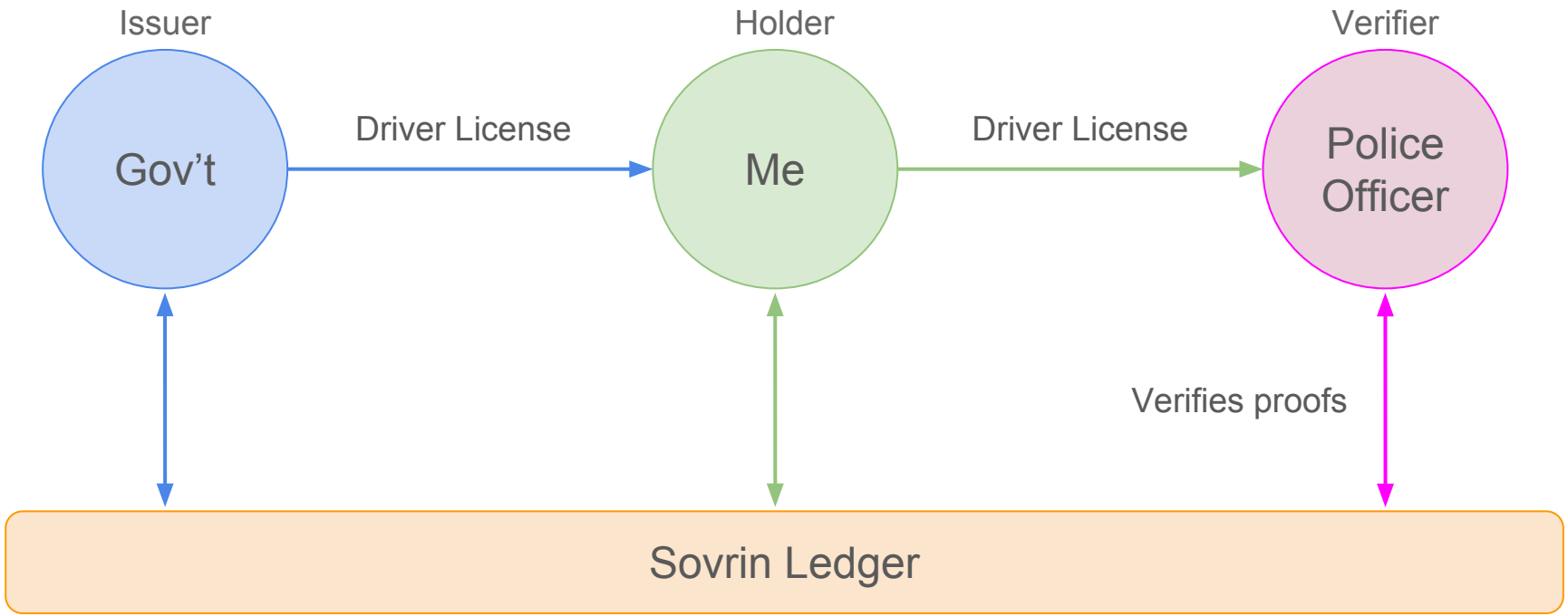
- Issuer: They create and issue credentials
- Holder: They receive, hold and share credentials with Verifiers
- Verifier: They receive and verify proofs (a digital sharing of all or part of a credential) from Holders


Issuer
Holder
Verifier
Issues Creds
Shares proofs
Verifies proofs
Sovrin Ledger

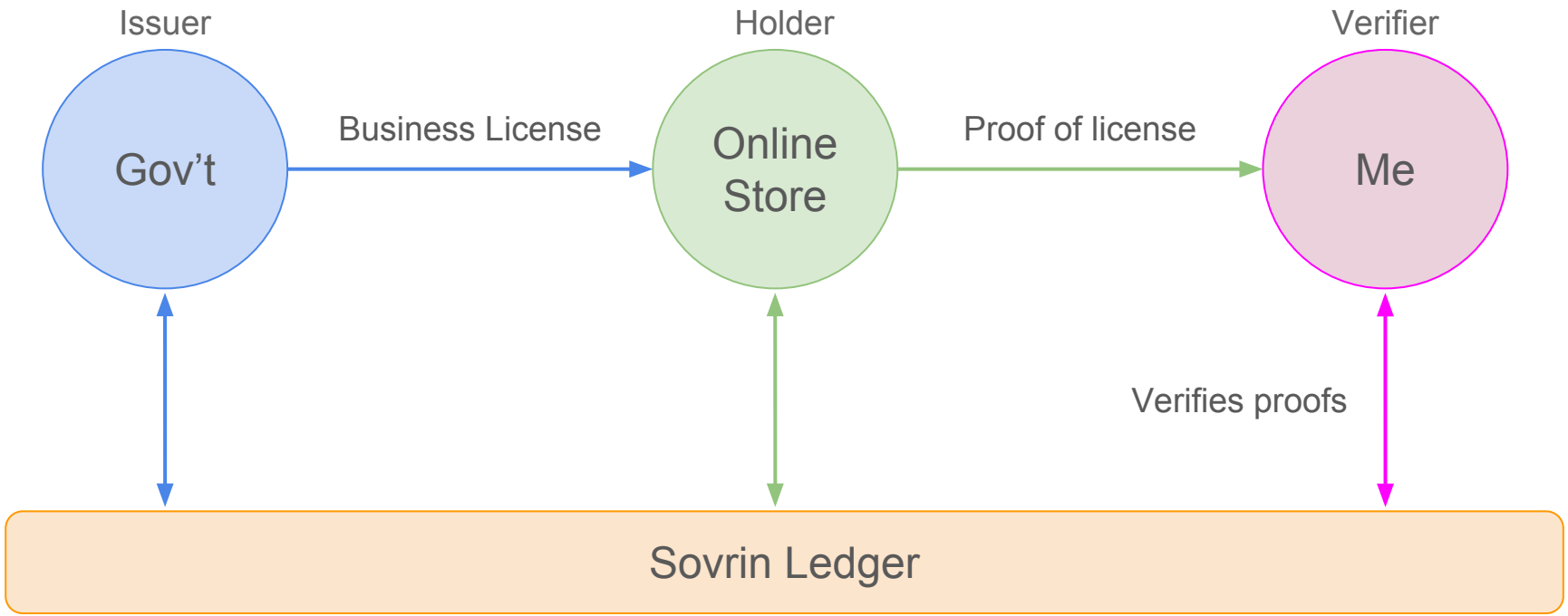
An Identity Owner can be all three



An Identity Owner can be all three

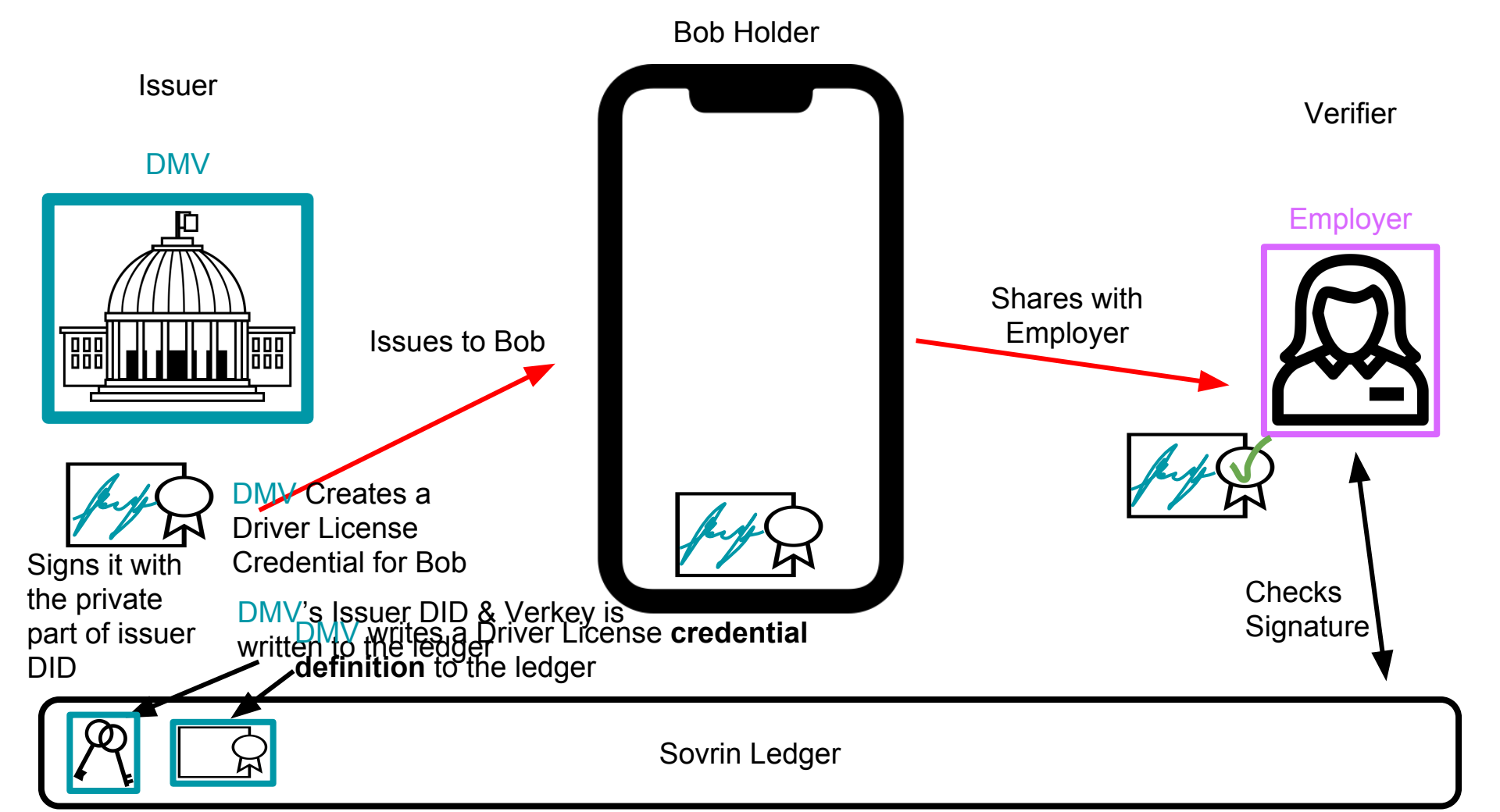


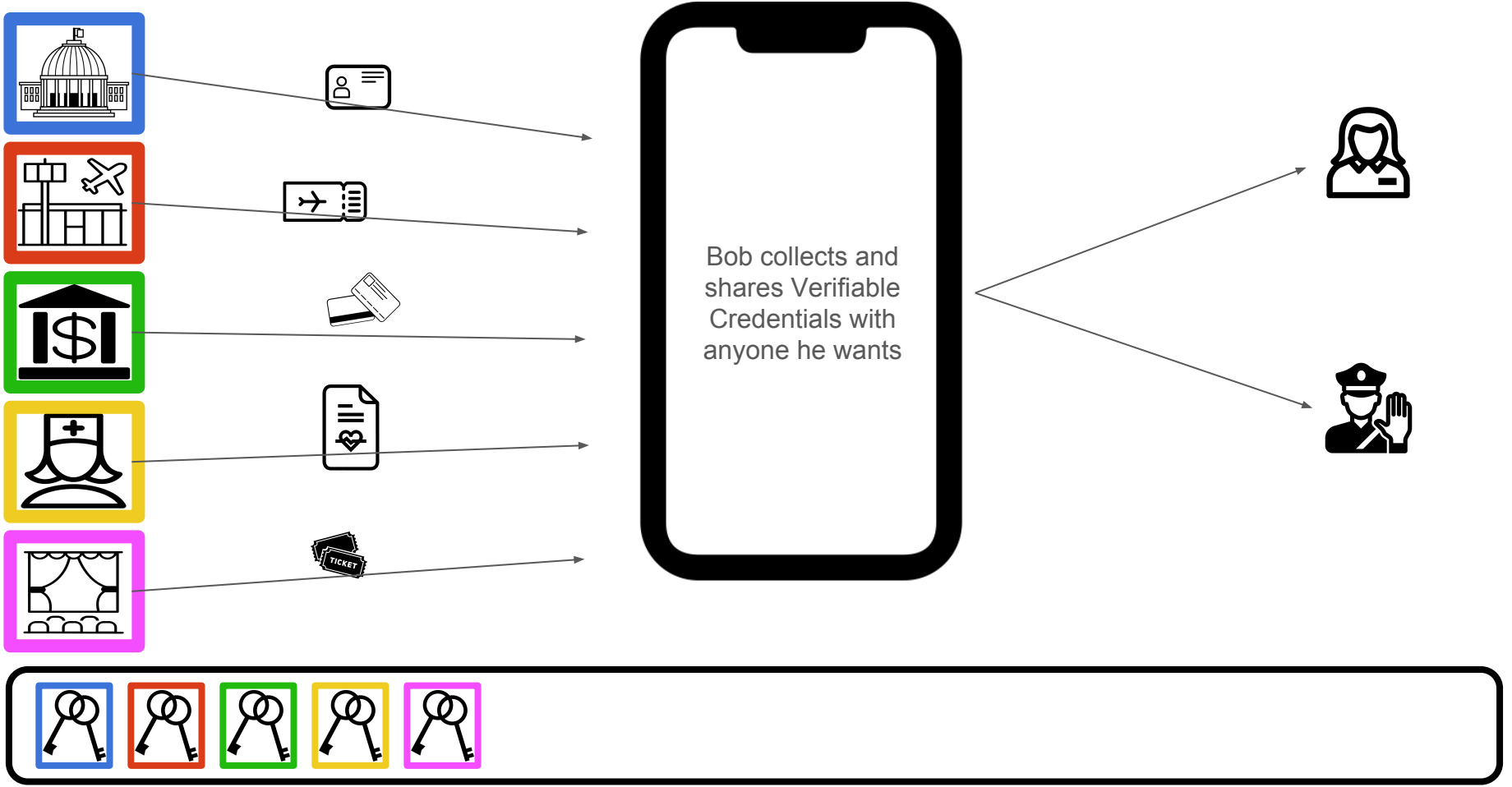
An Identity Owner can be all three



VCs use decentralized public key infrastructure

(DPKI)

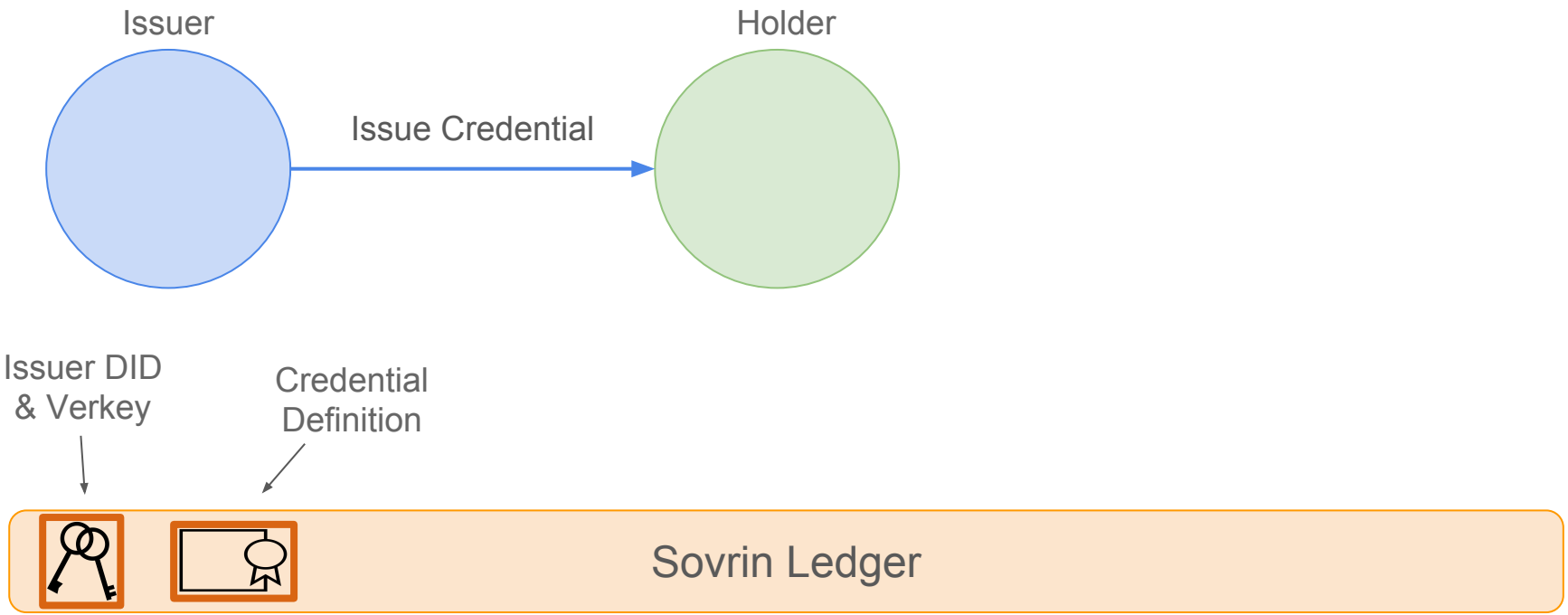

Bob Holder
Issuer
Verifier
DMV
Employer
Issues to Bob
Shares with Employer
DMV Creates a Driver License Credential for Bob
Signs it with the private part of issuer DID
DMV's Issuer DID & Verkey is written to the ledger
DMV writes a Driver License credential definition to the ledger
Checks Signature
Sovrin Ledger

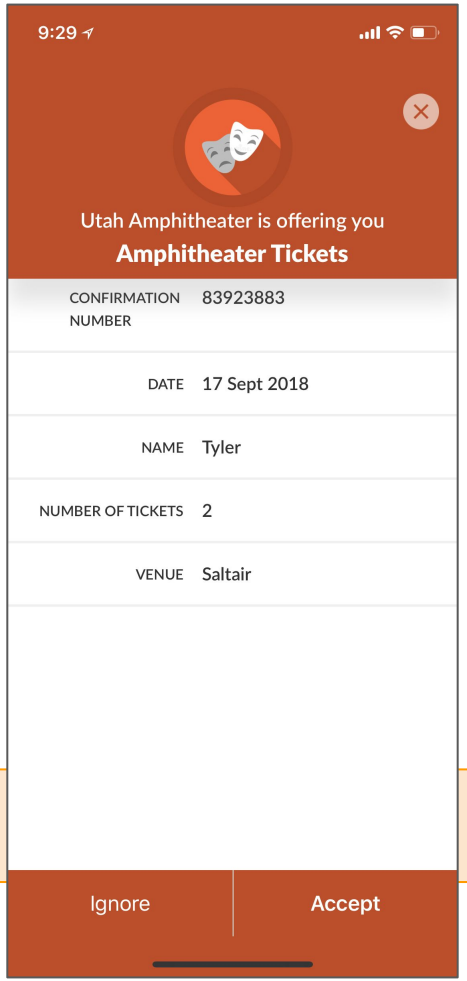

Bob collects and shares Verifiable Credentials with anyone he wants
TICKET

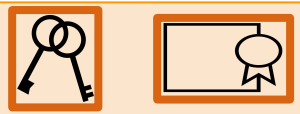
But how does a Verifier know a credential I share was *actually issued to me?*

What stops me from copying my credentials and sharing with all my friends?

Blinded Link Secrets

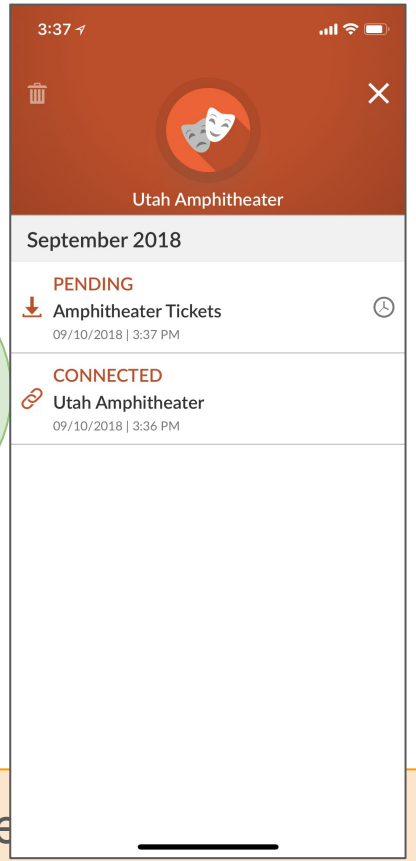

Issuer
Holder
Issue Credential
Issuer DID
& Verkey
Credential
Definition
Sovrin Ledger

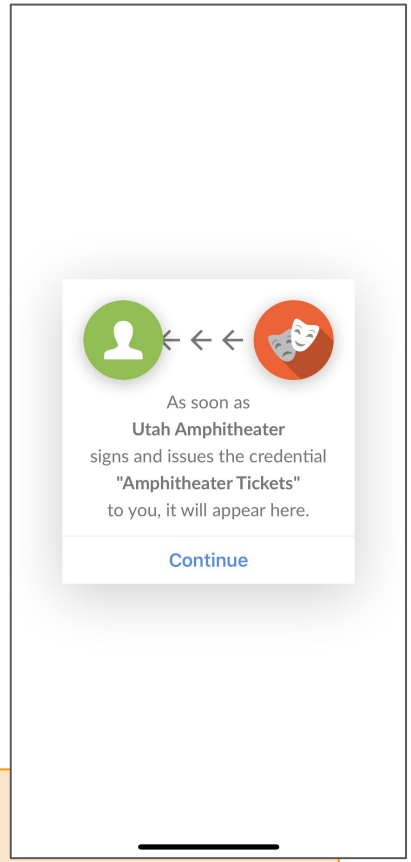


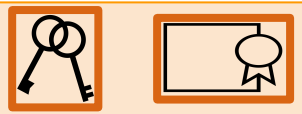


Sovrin Ledger

SSIMeetup.org







Sovrin Ledge

SSIMEETUP Self-Sovereign Identity

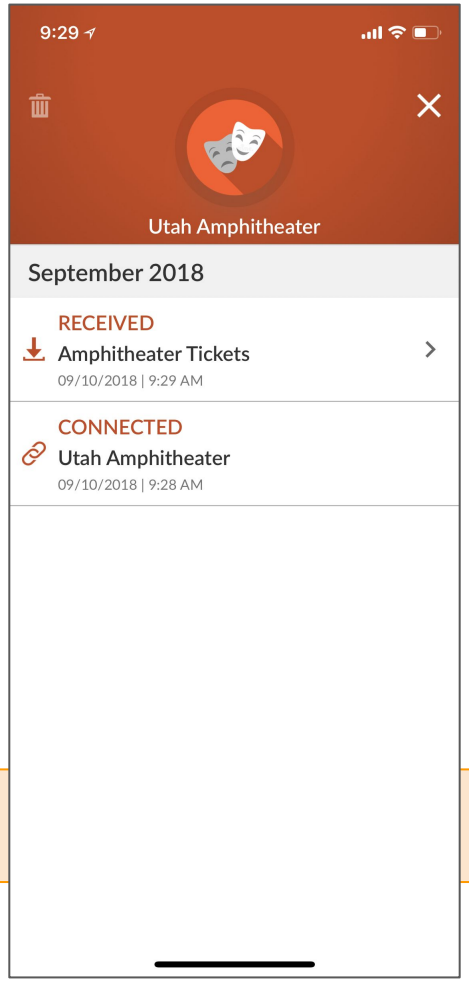
SSIMeetup.org

Issuer

Binds blinded link secret to credential

3. Issuance

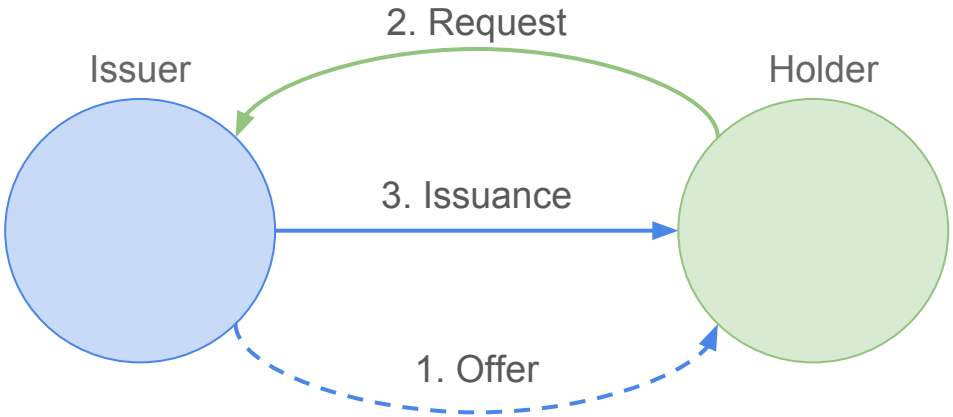
Holder

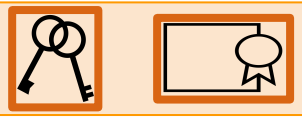


Sovrin Ledger

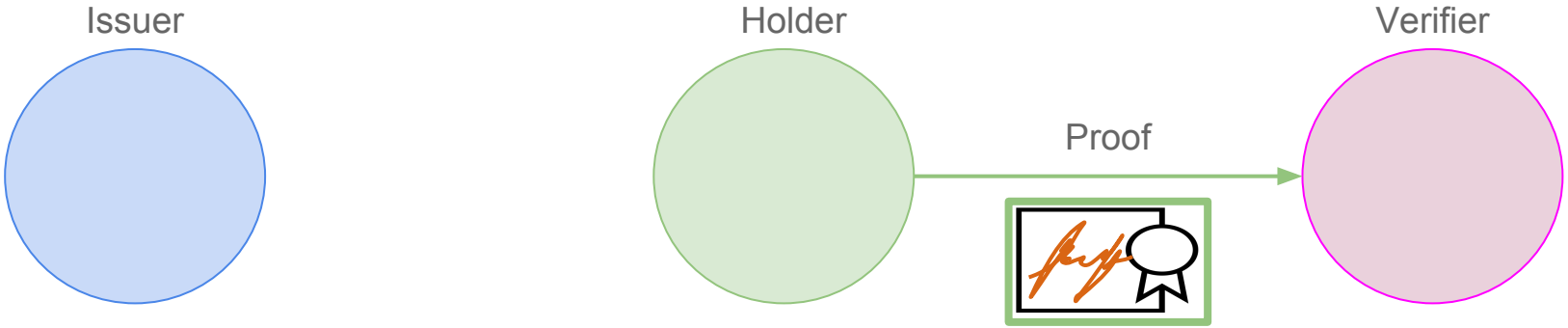
IMEETUP Self-Sovereign Identity

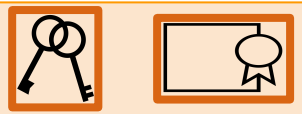
SSIMeetup.org





Sovrin Ledger





Sovrin Ledger

Issuer

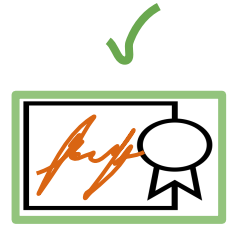
Holder

Verifier

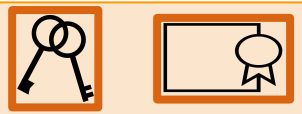
Sovrin Ledger

Issuer

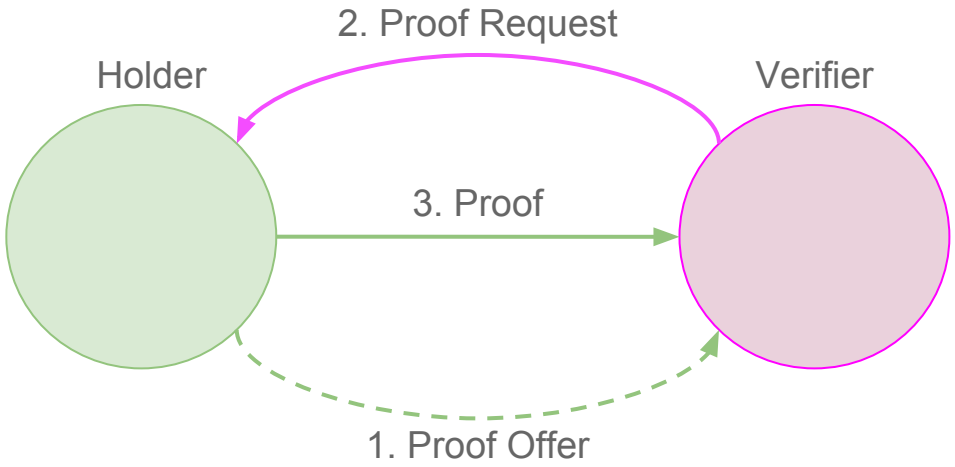
Holder



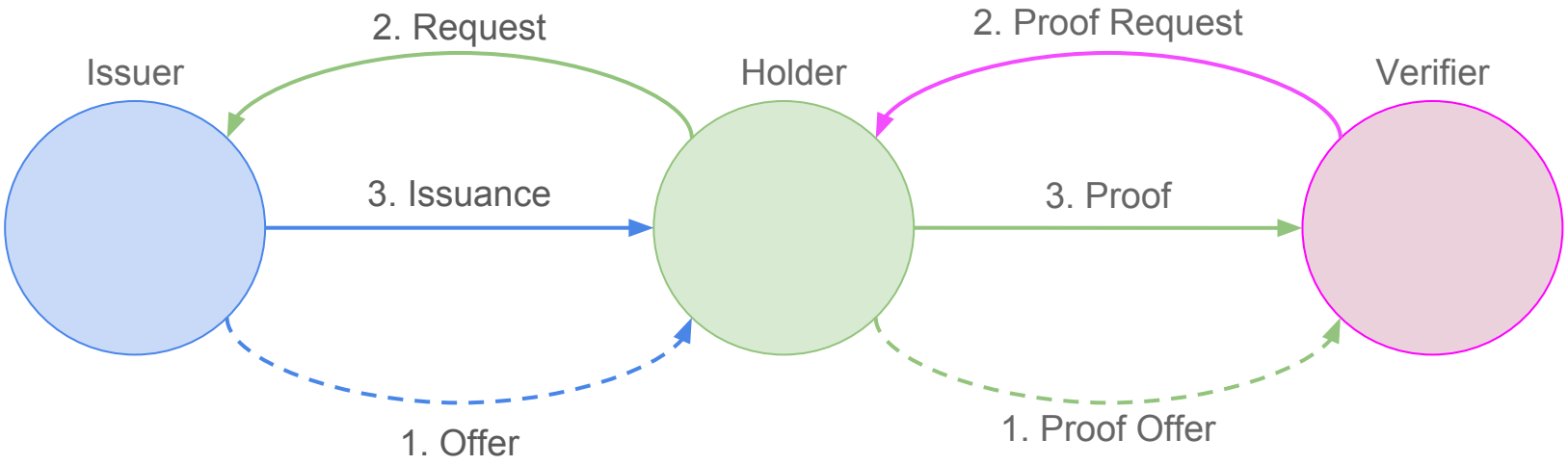
Verifier



Sovrin Ledger



Sovrin Ledger



Sovrin Ledger

SSIMEETUP Self-Sovereign Identity SSIMeetup.org

Verifiable Credentials are:

- All digital, under the true owner's control
- High scalability
- Much harder to fake
- Near impossible to impersonate true owner
- Eliminates need for any treasure troves of data
- Enables minimum disclosure
- Enables Zero-Knowledge Proofs
- Data alone is useless

Verifiable Credentials 101 for SSI

An intro and technical explanation

September 18, 2018

Tyler Ruff

Product Manager, Evernym

SSIMeetup.org