Privacy-Respecting Tech in Sovrin

Jason Law
Technical Governance Board Chair, Sovrin Foundation
Does Privacy matter?

- Maybe it doesn’t… until it does. Kind of like auto insurance?
- The problem is, we don’t know when it will matter.
- Even with advanced crypto, distributed ledgers can actually make privacy worse.
- The more we interact digitally, the more we ‘leak’ about ourselves.
- Years ago, if we wanted something, we would go to the market and buy something with a $10 bill, and our privacy was preserved.
Correlation (Linkability)

- Attribute-based Correlation
- Sharing too much
  - too many attributes (showing the whole driver license)
  - too much precision (birthdate instead of age, age instead of ‘over 21’)
- Identifier-based Correlation
- Signature or Hash-based Correlation
  - Even with selective disclosure
- Timing Inferences
  - Issuance correlated with verification (inspection)
- Among
  - Multiple relying parties
  - Between relying party and issuer
Hypothesis

- Hypothesis: Relying parties don’t necessarily want to know who you are; they want to know that you are authentic
- Correlation is a threat to Self-Sovereign Identity
- Interactions should be private by default
- Relying Parties don’t need to know so much
  - PII creates a liability for relying parties, e.g., GDPR
  - Disclosure creates inhibitions to engagement on a web site, limiting potentially rich interactions.
- When a technological solution is readily available, legislators will respond
Chaum, Camenisch-Lysyanskaya

- With advanced cryptographic signature schemes, you can...
  - Prove an attribute of a credential
  - Prove something *about* a credential
  - Prove attributes from two credentials from different issuers are for you
  - Prove that the credential is still valid and have not been revoked

- ...without disclosing who you are
  - or providing a strong point of correlation

- ...even if issuers and relying parties collude
  - think regime change
Anonymous Claims

- Implemented in Sovrin today
- Getting Started Tutorial gives an example of this.
- Not just for anonymity
- Even if you are ultimately identified, you don’t need to be identified against a single unique value that every other relying party knows.
- Progressive engagement (disclosing more and more with the opportunity to bail)
Revocation

- Proof of concept in the form of tests is in the Anoncreds repo at https://github.com/evernym/anoncreds
- Sovrin integration has been designed
- Will be implemented in Sovrin soon
How it works

1. Setup
2. Issuance
3. Proof Preparation
4. Verification

Issuer
Issues Claims

Identity Owner
Acquire, Store, Prepare Proofs

Relying Party
Requests Proof

Sovrin
Holds IDs, Keys, Public Attributes, Claim Defs, Issuer Keys, Revocation Info

write ID’s, Keys, etc.
verify ID’s

verify ID’s, claims

verify ID’s, proofs, non-revocation
Setup

1. An Issuer writes a Claim Definition
   a. which defines the name, version, and data structure or schema of the claims they will issue
   b. Example: Driver License, v1.0 (first_name: string, last_name: string, birthdate: date)

2. Issuer writes an Issuer Key
   a. Generates a special private/public key pair for that Claim Definition and writes the public part
      as an Issuer Key to Sovrin; is linked to the Claim Definition

3. Issuer writes a kind of summarized revocation list, called Validity Affidavit

4. Issuer writes a set of special revocation identifiers, called Validity Tails
   a. Pre-generates a number of random numbers to form Validity Tails
   b. Writes location(s) and hash of Validity Tails along with a special ‘accumulator’ or affidavit
Issuance

1. Identity Owner authenticates to Issuer
2. Identify Owner generates a master secret that is ‘sealed’
3. Issuer ‘signs’ the sealed master secret, a number of attributes, and some special revocation information.
   a. This is a Sovrin Claim, though it is not written to Sovrin.
4. Identity owner verifies the Claim
5. Issuer updates the Validity Affidavit, including special indices
   a. so that this new Claim can be proven to be valid
6. Identity Owner downloads the Validity Tails, and creates a Witness
   a. the witness is stored locally, and used for proving non-revocation
Proof Preparation

1. Identity Owner initiates interaction with a relying party
2. Disclosure requirements are negotiated
   a. RP: show me everything
   b. Owner: no
   c. RP: OK, show me proof of address within 3 months
   d. Owner: OK
3. Identify Owner ensures it has a Witness that is sufficiently ‘fresh’
   a. If not, it retrieves latest Validity affidavit, and indices since the last update
   b. Identity Owner uses this information to update its Witness
4. Identity Owner prepares a proof of the negotiated attributes, along with a proof of non-revocation
5. Identity Owner sends these to the relying party
   a. along with any pseudonymous self-claims the owner wishes to share
Verification

1. Relying Party verifies the proof using…
   a. Claim Definition from Sovrin
   b. Issuer Key from Sovrin

2. Relying Party verifies the validity proof (proof of non-revocation) using…
   a. Validity Affidavit from Sovrin