2020-06-01 Indy Contributors Call

Summary

Planned:

- Work updates:
    - Indy VDR
    - Indy Credx
    - Aries Credx
    - Aries Storage
- Enabling agents to work with multiple Indy networks

The call recording is available here: 20200601-Indy Contributors Call.mp4

Remember the Hyperledger Code of Conduct

Anti-Trust Policy

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Introductions

Attendees

- Stephen Curran (Cloud Compass Computing Inc.) <swcurran@cloudcompass.ca>

Related Calls and Announcements

- Identity Implementer Working Group call (Wiki Page) - every 2nd Thursday

Release Status and Work Updates

- Move from Sovrin Foundation infrastructure
    - Stalled - no resources
- Indy Node
    - June(?):
        - Replacing Indy Crypto with Ursa (Kiva)
        - More "rich schema" objects
        - Ubuntu 20.04 (Kiva)
            - Need to check additional dependencies:

⚠ Unable to render Jira issues macro, execution error.

- Indy SDK
    - June(?):
        - Indy VDR into LibIndy
        - Indy Credx into LibIndy
- Aries Shared Libraries
    - Aries Shared:
        - indy-vdr (Andrew Whitehead) https://github.com/hyperledger/indy-vdr
            - No progress
        - indy-credx - https://github.com/andrewwhitehead/indy-credx
            - No progress
            - To be moved to Hyperledger
        - indy-shared-rs - https://github.com/bcgov/indy-shared-rs
            - Shared features across indy-vdr and indy-credx
            - pack/unpack on Ursa (not libsodium)
            - To be moved to Hyperledger
        - aries-credx

      - https://github.com/sovrin-foundation/aries-credx-framework-rs
        - 6 most common attribute encodings (but not anoncreds 1 attribute encoding)
      - Can make a non-revocable credential and create proofs.
    - Aries Secure Storage initiatives:
      - Mike working on documentation and architecture as an Aries RFC (KMS architecture) and Ursa RFC (API)
        - PR is submitted: https://github.com/hyperledger/aries-rfcs/pull/440
      - Mike and Cam's work aries-kms-mayaguez - Postgres backend for credential storage https://github.com/sovrin-foundation/aries-kms-rs
        - Persistence work allows plugging in any database engine.
        - Focus is using an external enclave.
      - aries-kms-vostok
        - Andrew also working on something similar – async wallet on sqlite, Indy functionality re-imagined - storage implementation
  - Ursa
    - Revocation work 2.0 work

Meeting Topics

- Revocation 2.0
  - Meeting with Brent Zundel Mike Lodder Andrew Whitehead Stephen Curran
  - Review of merkle tree construction based on leaf nodes containing \{ Begin, End \} indices of unrevoked credentials
    - RFC PR in progress - Non-Revocation Range Tree
    - Prover given index for credential
    - Proves in zero knowledge each of: index, index > begin, index < end and leaf \{ Begin, End \} is in the tree
    - Together they prove that credential issued to the prover is one that is not revoked.
  - We know the merkle tree construction is fast and space-efficient for registries of 1M and possibly 16M credentials.
    - Test ran with Poseidon Hashing (slows hash, but speeds proof generation) vs. SHA256 - not as fast, but in range
    - Could also run tests with 4- or 8-ary trees.
  - TBD: How fast is the construction of the proofs and what proof style to use?
  - Questions about what ZK tech has been investigated?
- Dynamic Ledger Resolution - Presentation
  - Goal is an agent that can easily interact dynamically with multiple Indy ledgers with minimal effort by the agent owner.
  - Today: Apps are Sovrin MainNet, Sovrin Staging, Sovrin BuilderNet, BCovrin and others.
    - User manually selects which ledger to use in Mobile Wallets.
  - Future: Market forces will result in credentials rooted in multiple Indy ledgers.

Future Calls

Next call:

Future:

- Requirements questions:
  - IS-1099: anoncreds.prover_get_credentials_for_proof_req should return per-credential timestamp
    - Should we allow duplicate credentials from the same issuer?

Action items

☐ PR to RFC #0019 to compare pack/upack to msgpack (Sergey)

☐ Review the 61 cases of "unsafe" libindy calls and figure out if they are justified.