2020-05-04 Indy Contributors Call

Summary

Planned:

- IIW Update
- Work updates:
    - Indy VDR
    - Indy Credx
    - Aries Credx
    - Aries Storage
- Migrating from JIRA to GitHub Issues
- Migrating from Jenkins to GitHub Actions (or Azure Pipelines)
- Update on Revocation 2.0 - Merkle Tree Processing Tech Spike
- If time: BBS+ ZKPs and Indy

The call was recorded is available here: 20200504 Indy Contributors Call

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>
- Brent Zundel (Evernym, Inc.) <brent.zundel@evernym.com>

Related Calls and Announcements

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

Release Status and Work Updates

- Move from Sovrin Foundation infrastructure - Wade Barnes
    - Move from Jenkins to GitHub actions
        - Sovrin Foundation Jenkins machines are going away
        - Sovrin resource migration
        - #cicd discussion "Indy CI / CD Migration" (in #cicd use menu item "Discussions" to see/get to the discussion)
    - Move repo.sovrin.org Hyperledger Artifactory for all except Sovrin Foundation specific artifacts
- Indy Node
    - April: no release
    - May:
        - 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
    - April: no release
    - May/June:
        - Indy VDR into LibIndy
        - Indy Credx into LibIndy
- Aries Shared Libraries

- Aries Shared:
    - indy-vdr (Andrew Whitehead) https://github.com/hyperledger/indy-vdr
        - Nearing release 0.6(?) - most work complete that was needed: Design doc, FFI, testing, CI / CD
            - CI - GitHub actions runs unit tests and basic integration tests
            - CD not there
            - No design doc, but crate docs
            - Rich Schema merged and behind a feature flag
            - Refactoring PR not merged - cleanup, internal simplification, crate docs
        - As an Aries interface becomes standardized, will add that API layer
        - VON Network browser moved to Indy-VDR - branch
        - BC Gov created a tails server based on Indy-VDR - with dynamic ledger access
    - indy-credx - https://github.com/andrewwhitehead/indy-credx
        - need to move ASAP to at least BC Gov repo - Andrew Whitehead
        - ACA-Py branch created that can do credential exchange with indy-credx
        - Next up: adding revocation 2.0 support
        - Integrating upgraded PyO3 library
    - indy-shared-rs - https://github.com/bcgov/indy-shared-rs
        - Shared features across indy-vdr and indy-credx
        - pack/unpack on Ursa (not libsodium)
        - home for revocation support? Or at least shared set membership proof handling?
        - Move to Hyperledger move this week...
    - aries-credx
        - https://github.com/sovrin-foundation/aries-credx-framework-rs
            - 6 most common attribute encodings
            - Does not have anoncreds 1 attribute encoding.
        - Can make a non-revocable credential and create proofs.
            - Tagging will be moved to the KMS.
            - Mike will be working on revocation registry 2.0
    - 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.
- Ursa
    - BBS+ added
    - 0.3.5 pending, plus new additions

Meeting Topics

- IIW
    - BBS+
    - DIDComm and CHAPI Discussion
- Update: Move to GitHub Issues from JIRA for indy-sdk, indy-node, indy-plenum
    - Issues now active
    - Pending: Putting in the PR to announce location of issues in READMEs
- Update: Migrate Jenkins to GitHub Actions (and perhaps Azure pipelines)
    - Plan started - Sovrin resource migration
    - Resources: Wade Barnes (BC Gov), Thor Wolpert (BC Gov) for first step (Indy SDK/Linux)
- Revocation 2.0 - Tech Spike on Merkle Trees in process (Daniel Hardman)
    - Tech Spike Implementation: https://github.com/dhh1128/merklespike
    - Notes on Issues: size of compressed leaves, resources to calculate internal nodes
    - Next steps - continue with the spike
    - Side note: Digital Bazaar is using a bit field as non-ZKP revocation registry
- BBS+ Signatures enables ZKPs with JSON-LD
    - Draft Spec: http://mattrglobal.github.io/jsonld-signatures-bbs-spec/
    - Draft spec repo: http://github.com/mattrglobal/jsonld-signatures-bbs-spec
    - BBS+ signature implementations: https://github.com/mattrglobal/node-bbs-signatures https://github.com/andrewwhitehead/ursa-bbs-py
    - JSON-LD signature suite to use with VC-JS: http://github.com/mattrglobal/jsonld-signatures-bbs
    - Regarding credential schema definitions in the vc data model: http://w3c.github.io/vc-data-model/#data-schemas
    - Proof formats in the VC Data Model: http://w3c.github.io/vc-data-model/#proof-formats
    - The paper for “provable security”: http://eprint.iacr.org/2016/663.pdf
    - Next steps:
        - Revocation - credential status field
        - Predicates?
        - CCG - being put forward by Mattr
        - Question: How does required reveal work at the crypto layer?

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.

Call Recording

? Unknown Attachment