# 2020-01-13 Indy Contributors Call

## Summary

- Work updates
- Results from performance testing LibIndy
- INDY-2305 and outbound IP address

## Timezone: Europe afternoon / America morning

## We intend to record this 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

- Name (Organization) <email>
- Richard Esplin (Evernym) <richard.esplin@evernym.com>
- Alexander Shcherbakov <alexander.shcherbakov@evernym.com>
- Ken Ebert (Sovrin Foundation) <ken@sovrin.org>
- Cam Parra (Kiva) <camilop@kiva.org>
- Daniel Bluhm (Sovrin Foundation) <daniel.bluhm@sovrin.org>

## Related Calls and Announcements

- Previous Indy Contributors call was cancelled
- Identity Implementors Working Group call
    - Main place to get project updates, release status, and announcements.
- Recording and slides are posted for the SSI Meetup webinar on Indy and Plenum.

## Release Status and Work Updates

- Indy Node
    - December: 1.12.1
        - Improvements to the TAA behavior
        - Roll-out to Sovrin Network delayed: Post-release identified corner cases related to View Change, and weirdness seen during Builder Net upgrade. Investigation is ongoing.
    - January:
        - Additional rich schemas objects: schema object (Sovrin Foundation)
            - Just posted Indy HIPE https://github.com/hyperledger/indy-hipe/pull/149
            - Aries RFC https://github.com/hyperledger/aries-rfcs/pull/281
            - PR of schema object in progress for December
            - Making progress on other RFCs for objects and one that shows how all the objects fit together.
            - Next: encoding object, then mapping object
        - Replacing Indy Crypto with Ursa (Kiva)
            - Debian packages for Ursa-0.3.0 are uploaded to repo.sovrin.org
    - Future
        - Ubuntu 18.04 (Kiva)

      - Need to check additional dependencies:

⚠ Unable to render Jira issues macro, execution error.

    - Remove replicas (Aardvark BFT) ?
    - Anoncreds 2.0 (Sovrin Foundation)
- Indy SDK
  - December: 1.14.0 / 1.14.1
    - LibVCX support for Aries Interop v1
    - Improvements to the TAA behavior
  - January:
    - Bugfixes
  - Future
    - Deprecating some docs (IS-1425: Getting Started Guides) and wrappers (IS-1423: Python and DotNet)
    - Deprecate  additional wrappers (IS-1424) and LibVCX (IS-1416)
    - GitLab migration alongside Jenkins (Foundation)?
    - Warnings from rust cargo clippy (Mike and Axel), epic: IS-1401
- Indy Catalyst
  - Plan is to moving to aries-verified-credential-registry
  - https://github.com/bcgov/indy-catalyst
  - Production deployment testing: volume loads.
    - Happy with performance now.
  - Not yet migrated to Hyperledger. Needs more documentation.
- New design for revocation / Anoncreds 2.0 (Mike)
  - Would be useful to have a comparison in performance between Anoncreds 1.0 and Anoncreds 2.0
  - Need a plan for changes to Indy Node
    - HIPE for overall changes, then a design PR for the changes specific to the different repos. https://github.com/hyperledger/indy-node/tree/master/design
    - BC.gov will implement the existing revocation capability in ACA-Py for use in constrained cases
      - Looking to build against Anoncreds 2.0 as soon as it is available.
      - Unable to contribute to the Anoncreds 2.0 revocation capability at this time - no resources for that work.
- Aries Shared Libraries
  - indy-aries-vdr (Andrew Whitehead)

## Main Business

- Kiva update:
  - test networks is running Indy Node 1.8
    - Seeing some compatibility issues
  - created 5 million test wallets with citizen data
- Non-secrets in the Indy Wallet
  - Cam is working on pluggable crypto. The wallet shouldn't decide what encryption you should be using.
    - https://github.com/mac-arrap/aries-rfcs/tree/master/concepts/0276-key-management-service
    - Indy wallet currently forces encryption to avoid mistakes in the ecosystem, specifically around searching
  - Best practices with Indy today
    - Indy wallet wasn't designed for general storage, but people are using it because there aren't alternatives.
  - Shared goals for Aries
    - Aries-KMS is key specific
      - link secret should be treated the same as a key
    - Separate storage for connections, credentials, and protocol state
    - Need an additional storage for larger items
- Use cases where we would want to move keys between wallets
  - We receive requests for moving the link secret / credential data from one device to another (synchronized storage)
    - Concerns with private keys ever leaving the wallet. If it can be done for any use case, how can it be protected against malicious use cases?
    - But wallet portability requires migration: export from one wallet, and import into a different wallet
      - migration between vendors
      - some types of upgrades
    - Preferred approach is to create a protocol for migrating credentials between wallets: move data and rotate to new private keys.
      - How do we handle the link secret?
  - Related use cases
    - backup and restore: storage layer backup
    - Debug use cases: unencrypted wallet plugin?
    - Delegation and guardianship: DID Doc
    - Enterprise use case:  pre-signing, signing API for arbitrary data.
  - Work-around with the web-crypto API

## Future Calls

- Results from performance testing LibIndy (BC.gov)
- Requirements questions:
  - INDY-2305: Add IP address range for outbound TCP connections from validator nodes
    - Changes the way nodes are represented in the Pool Ledger
  - 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

- ☐ HIPE #138, Issue #144 (Ken and Brent)
    - Create a PR for changing status to ACCEPTED
    - Check for an Aries RFC
- ☐ PR to RFC #0019 to compare pack/upack to msgpack (Sergey)
- ☐ Richard and Sergey will close old pull requests with a descriptive comment.
- ☐ Mike wants to review the 61 cases of "unsafe" libindy calls and figure out if they are justified.

## Call Recording

zoom_0.mp4