

2020-02-24 Indy Contributors Call

Summary

- Work updates and collaboration on projects
 - VDR
 - CredX
 - Rich Schemas
- Future of Indy CI / CD

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>

Related Calls and Announcements

- Going forward, we will not be holding the AMER afternoon / APAC morning call
- Identity Implementors Working Group call
 - Main place to get project updates, release status, and announcements.
- Call to discuss techniques for supporting an Indy Network: Tuesday, February 25 at 3PM UTC

Release Status and Work Updates

- Indy Node
 - February:
 - No formal release of Indy Node
 - New items available
 - Tool for detecting ZMQ network problems
 - Troubleshooting guide
 - March:
 - Replacing Indy Crypto with Ursa (Kiva)
 - More "rich schema" objects
 - Future
 - Ubuntu 18.04 (Kiva)
- Need to check additional dependencies:
- Indy SDK
 - February:
 - 1.15.0:
 - LibVCX improvements to reject proof and connection redirect
 - Bug fixes
- Indy Catalyst
 - <https://github.com/bcgov/indy-catalyst>
 - Still working on performance improvements
 - Being deployed at Government of Canada
 - Migrating to Hyperledger Aries: plan is to moving to aries-verified-credential-registry
 - Needs more documentation




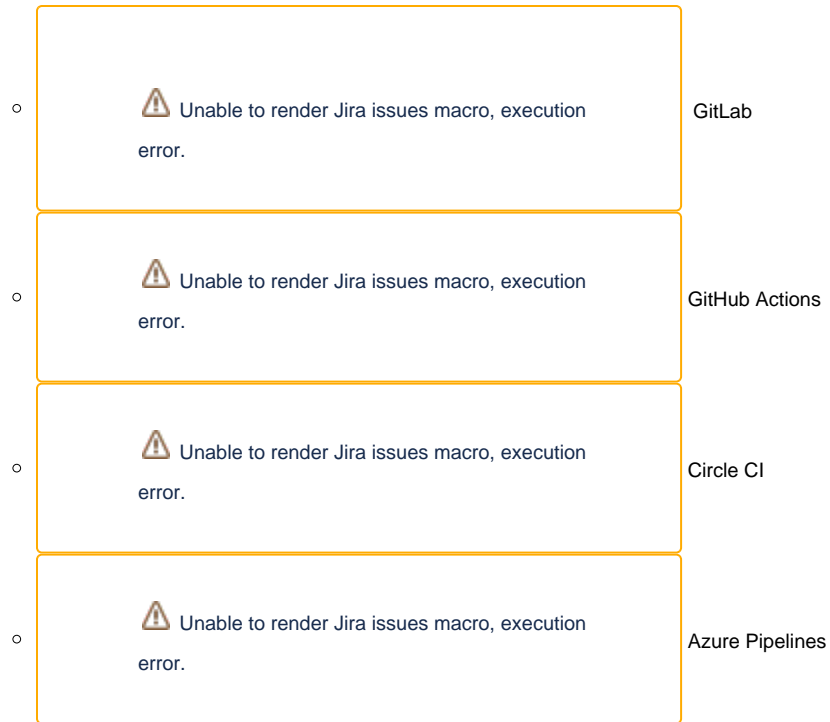
Unable to render Jira issues macro, execution error.

- Anoncreds 2.0 (Mike)
 - Implementing in an Aries Shared Library
- Aries Shared Libraries
 - indy-vdr ([Andrew Whitehead](https://github.com/andrewwhitehead/indy-ledger-client)) <https://github.com/andrewwhitehead/indy-ledger-client>
 - HTTP REST client that can be used to proxy ZMQ traffic
 - Next steps:
 - VDR Design Doc
 - Custom State-Proof Parser
 - Currently uses global state, should use an object (currently commented out in Indy-VDR)
 - Pair-programming session: BC.gov team, Adam B, Ev Team
 - FFI
 - Unit tests
 - Functional tests
 - Migrate repo to Hyperledger
 - First commit should point to previous history in indy-sdk
 - Integrate into existing LibIndy
 - Apply recent bug fixes to the new VDRI
 - As an Aries interface becomes standardized, a new repo will be created for the indy-aries-vdri
 - Or a single aries-vdri with modules for each interoperable ledger
 - indy-aries-anoncreds / indy-creds indy-credx
 - Mike has started. Repo for Aries cred exchange framework. <https://github.com/sovrin-foundation/aries-credx-framework-rs>
 - As an Aries interface becomes standardized, a new repo would be created for the indy-aries-credx?
 - Goal is to make the current anoncreds a separate component, then work on anoncreds 2
 - Microsoft might be taking a different approach to ZKPs <https://eprint.iacr.org/2019/550.pdf>
 - Aries-Shared-Util
 - Pack / Unpack
 - Lift-and-shift would be Indy specific, but refactoring for Aries-KMS could take a long time
 - Need a place for Rich Schemas functions many will go to Aries Credx
 - Aries-KMS
 - Mike and Cam's aries-core-rs aries-kms-(placeholder) <https://github.com/sovrin-foundation/aries-core-rs>
 - Evolution from lox
 - Will include a default storage that is not a different implementation from the plugins
 - Hopes for a prototype in February
 - Move the Indy wallet crate as a starting point aries-kms-taiga
- Ursa 0.3.2
 - Releasing this week?
 - Implements key exchange, so LibSodium hopefully is no longer required

Main Business

- Connection Redirect
 - Evernym has something working in LibVCX, and needs to contribute an Aries RFC
 - Stephen, George, Sam, and Andrew are working on a similar Aries RFC
- Indy-Credx
 - <https://github.com/andrewwhitehead/indy-credx>
 - Using Pyo3: Python extension written in Rust that wraps crate directly. Improves performance and security. Allows multiple threads.
 - Expect to add an FFI interface in the future
 - Can issue credentials, no support for proof requests or revocation yet
- Indy-VDR
 - Making progress on tests
 - Want to add to VON Network
 - Has a fix for a problem with attrib transactions not being hashed into the state proof
 - https://github.com/andrewwhitehead/indy-vdr/blob/414b1903c2a9efb99ee2a9e6c844394f822ca094/libindy_vdr/src/state_proof/mod.rs#L1182
- "State proof" validation bug reported through the HTTP Proxy: audit ledger proof

 Unable to render Jira issues macro, execution error.
- Need to decide the future of CI / CD
 - Need CI / CD for indy-vdr immediately
 - Does the team at BC.gov have plans?
 - Indy-VDR has a docker that can be used for tests
 - Want to create a GitHub action
 - Where should it live?
 - Current Jenkins infrastructure is aging
 - Foundation's GitLab environment isn't functional
 - Hyperledger is using Azure Pipelines, but concerns about running an Indy Pool there
 - Evernym team's recent research:



- Ursa doesn't have any CI
 - Decided: Move forward with GitHub Actions
- Rich Schemas:
 - Need to correct existing HIPEs
 - Need to evolve DIF DIDComm to support Rich Schemas
 - Implement first in Indy-VDR and Indy-Credx, then decide how to migrate there from LibIndy.
 - How will we mix old credential definitions with new credential definitions?
 - Only difference is the mapping object
 - Anoncreds 1.0 vs 2.0 might require more effort to remain compatible. Anoncreds 2.0 only support Rich Schemas (new credential definition object)?

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

- ☐ 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



audio_only.m4a