# 2020-06-10-B Aries Working Group Call (US afternoon)

## Summary:

- Machine Readable Governance Framework
- OOB Progress / Updates

## Note: This call was recorded: <To be inserted>, Chat: 20200610 Aries WG B - Zoom Chat.txt

However, there was no screen sharing on the meeting.  The links for the presentations are provided below in the Agenda section.

## Date

10 Jun 2020 (12PM Los Angeles, 3PM New York, Tuesday at 7AM Sydney)

## 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.

## Attendees

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

Steve McCown (Anonyome Labs) <smccown@anonyome.com>

## Welcome / Introductions

## Announcements

## Related Meetings Review

- Ursa -
- Semantics - Next meeting: Never - transitioning to be in the ToIP Foundation - see RocketChat channel for details and how to join the successor group
- DID UX Call - Active?
- SSI in IoT WG
- Indy Contributors - Next Monday - Release Process and update, Namespacing Update, Revocation Update, Other?
- Identity WG / Identity WG Implementer calls (Wed / Thurs) - Next on is next week
- DIF DIDComm WG - Monday's at Noon US/Pacific - Sam Curren (Mon) - DID Doc services, etc.

## Upcoming Releases and Work Updates

- Aries Protocol Test Suite
    - Instructions, docker added - Try It!
    - Issue, credential, and proof tests are merged.
- Aries Agent Test Harness - https://github.com/bcgov/aries-agent-test-harness
    - Test compatibility between any two agents
    - Work on Present Proof tests.  Adding 4th agent personna (Acme, Bob, Faber and Mallory)
    - Bounty for implementing the Aries Framework .NET backchannel (and maybe others) – Apply Now
- Aries Shared:
    - Aries Shared:
        - indy-vdr (Andrew Whitehead)  https://github.com/hyperledger/indy-vdr
            - **Help Wanted**: Update `did:sov` method of the universal resolver to use indy-vdr instead of indy-sdk
        - indy-credx - https://github.com/bcgov/indy-credx
            - Experimental ACA-Py branch created that can do credential exchange with indy-credx
        - indy-shared-rs - https://github.com/bcgov/indy-shared-rs
            - Shared features across indy-vdr and indy-credx
            - pack/unpack on Ursa (not libsodium)
        - aries-credx-framework-rust - https://github.com/sovrin-foundation/aries-credx-framework-rs

- Aries Secure Storage initiatives:
  - Soon to be pubic - from Andrew Whitehead
- Aries-CloudAgent-Python (bc.gov)
  - Release 0.5.1 is on PyPi.
  - Looking at enhancing the revocation support work - less effort for controller, more on ACA-Py
  - OOB support being added
  - Initial JSON-LD VC support added – signing, verifying only - done by Sam Curren supported by SICPA (Switzerland)
- Aries-Framework-Go (Troy) #aries-go
  - Implementing the Out-Of-Band protocol
  - Implementing issue-credential and present-proof protocols
  - Edge agent in work based aries-framework-go using WASM with support for DIDs, VCs and DIDComm support being added
- Aries-SDK-Ruby (Jack)
  - Added DID/Verkey sign_and_submit to aries_sdk_ruby and published new gem (0.0.8)
  - Created aries-rails-docker experiment that support Rails 4 with Indy 1.8.1 on Heroku & Dokku
- Aries-Framework-DotNet (Tomislav)
  - BBS+ support added - a wrapper.  Tech spike work. https://github.com/streetcred-id/bbs-signatures-dotnet
- Aries-StaticAgent-Python
- Aries-Toolbox
  - PR for Connections Update
  - Converted to a web application by Robert Mitwicki - repo https://github.com/thclab/aries
  - Upcoming cleanup items
- Aries-SDK-Java
- Aries-Framework-JavaScript - Framework JS Meetings
  - Current focus is on mediator use case (NodeJS)
  - Plan for 1.0 defined; refactoring to be done
- Rich Schemas and W3C Verifiable Credentials (Brent & Ken)
  - Some work has been done to support the W3C Verifiable Credentials Data Model specification
- Aries-MobileAgent-Xamarin (Aries MAX) - https://github.com/hyperledger/aries-mobileagent-xamarin
  - Ideas:
    - Automatic offer acceptance/managing credentials
    - Machine readable governance
- Ursa
  - To replace libsodium, need to have a replacement for the anoncrypt / authcrypt sealed box for pack / unpack.
    - Can be done in Ursa with two steps, but might add as a single function call.
  - Revocation 2.0 Support - new approach: Non-Revocation Range Merkle Tree - Ursa RFC here
    - Performance looks good at 1M creds/registry - 16M might be possible.

# Agenda

- Intro and project updates (Stephen Curran  - 20 min)
- Machine Readable Governance Frameworks (Daniel Hardman  20 min) - RFC 430
- Out of Band Updates (Stephen Curran15 min)
  - Presentation
  - PR for RFC 0496 (Community Coordinated Update)
  - PR 499 for table outlining use case for OOB message receiver
  - Issue 497: put `reuse` in OOB protocol
  - Request for Help on Issue 470 - URL Shortener
- Open Discussion / Next Week Topics / Wrap Up (5 min)

# Next Week

- Requests?

# Future Topics

- Aries Storage ideas - Andrew Whitehead
- Migrating to new JWE envelope format: https://github.com/hyperledger/aries-rfcs/issues/478
- DKMS status
- Credential Fraud:  Example how in ACA-Py to verify same link secret across multiple credentials in presentation
- Schema interop - how to reuse a schema across different networks Robert Mitwicki(RFC in progress)
- Using WebSocket as a way to communicate back to the mobile/desktop wallet (Agent (services or user) as a proxy for communication between service and digital wallet) Robert Mitwicki

# Action items

- Pursue idea of "reuse" in OOB Protocol and remove from DID Exchange

| File | Modified |
| --- | --- |
| Multimedia File GMT20200610-185636_Aries-WG-C_640x360.mp4 | Jun 17, 2020 by Sam Curren |
| Multimedia File GMT20200610-185636_Aries-WG-C.m4a | Jun 17, 2020 by Sam Curren |