2019-12-04-B Aries Working Group Call (US afternoon)

Summary:
This meeting was during the connectathon, and due to low attendance, the agenda was deferred to next week.

Note: This call is being recorded.

Date
04 Dec 2019 (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
- Name (Organization) <email>
  - Troy Ronda (SecureKey) <troy.ronda@securekey.com>
  - Robert Mitwicki <robert@thclab.online>

Welcome / Introductions

Announcements
- Aries Workshop/Connectathon December 3-5 in Provo, Utah (On Now!)
- New Indy/Aries/Ursa edX course, now online - enroll now!
- Dec 25th and Jan 1st calls Cancelled for holidays(?)

Related Meetings Review
- Ursa - Progress on packages and Plenum work.
- Semantics - ODCA pilots underway - The agenda, video, notes, etc. from the HL Indy Semantics WG call:
  - Read more: https://odca.online and https://tool.odca.online
  - Fully functional parser: https://github.com/THCLab/odca-ruby
- DID UX Call - Slack/Mailing list - details in the shared document as well minutes and additional information, currently focus on Purpose Based Services
- SSI in IoT WG
- Indy Contributors - Richard Esplin (Mon) - Discussed future of Indy Ledger (View Change, Aardvark BFT, bug fixes, future of Plenum)
- Identity WG / Identity WG Implementer calls (Wed / Thurs)

Upcoming Releases and Work Updates
- Aries-KMS
  - Moving Indy Wallet crate into aries-ams / aries-kms (might change the repo name)
  - cam's rust aries-kms (just old code in repo right now, once I add more to my RFC I will focus my attention to adding code here)
- Working on aries-kms RFC
- Verifiable Data Registry Interface library
  - Ken's POC
- Other Core Libraries (pack / unpack)
- Aries-CloudAgent-Python (bc.gov) - Latest is Release 0.3.5 on PyPi - no code releases. Release 0.4.0 is likely next, which will have some breaking changes.
- Aries-Framework-Go (Troy) #aries-go
  - Weekly planning notes (2019-12-03).
  - Working on mediator/routing, WebSocket transport, WASM, browser primitives, JWE envelope.
- RFC efforts WIP from aries-framework-go contributors:
  - JWE envelope
  - HTTP over DIDComm
- **DIDAuthZ**
- Aries-SDK-Ruby (Jack)
  - No update this week
- Aries-Framework-DotNet (Tomislav)
- Aries-StaticAgent-Python - 0.7.0
- Aries-Toolbox
  - Moving repos to HyperLedger's Github Org.
  - ACAPy plugin for supported admin protocols.
- Aries-SDK-Python - Wrapper from JeromK and SBCA?
- Aries-Framework-Java #aries-framework-java on RocketChat
- Aries-SDK-JavaScript
  - PR for moving Indy NodeJS wrapper repo has been merged into https://github.com/hyperledger/aries-framework-javascript
  - Repo is ready for contributors to start picking next tasks
  - Regular weekly zoom calls to be scheduled from this Friday. Will share the details on Rocket Chat.
  - DIF people interested in implementing a Java Script library that might share some of the functionality of the Aries SDK. We need to keep that in mind.
- Rich Schemas and W3C Verifiable Credentials (Brent & Ken)
  - HIPEs/RFCs
    - overview https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0250-rich-schemas
    - context https://github.com/hyperledger/aries-rfcs/tree/master/features/0249-rich-schema-contexts
    - schema processing feedback https://github.com/hyperledger/aries-rfcs/tree/master/features/0281-rich-schemas
  - Next HIPEs/RFCs for
    - encoding
    - mapping
    - credential definition
  - Node implementation of
    - context (merged)
    - schema PR in progress https://github.com/hyperledger/indy-node/pull/1513
- Migration from LibIndy
  - Closing PRs related to Indy wrappers with pointers to Aries language libraries
  - LibVCX support for some Aries protocols
- Ursa 0.3.0 release in November
  - Updated BLS signature (multi-signatures, small-BLS)
  - Compilation optimization for specific hardware
  - Rest of predicates for Anoncreds 2.0 and delegatable credentials

**Agenda**

- Issue Game: Can we close this? (15 min - Sam Curren) - issues (as time permits): #198, #130, #41, #114
- Connectathon Update
  - Aries Interop Profiles
  - Testing
    - Single Agent / Multi-Agent
    - Backchannels
- Use of please_ack in the issue_credentials protocol (15 min - Stephen Curran) - presentation
- Open Discussion / Next Week Topics

**Next Week**

**Future Topics**

- DIF Interop Project - Project is proceeding, connect the communities at IIW
- DKMS status
- Independent agent upgrades
- Signature Envelope (Kyle)
  - Updating to JWE compliant data model
- Credential Fraud: Example how in ACA-Py to verify same link secret across multiple credentials in presentation
- Schema interoper - how to reused 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
- Update message type and protocol identifier to https. (and protocol documentation hosting.)
- Formal protocol verification techniques
  - https://github.com/johncallahan/needham_shroeder_spin (non-Aries example using SPIN/Promela)

**Action items**

**Call Recording**