2019-11-20-A Aries Working Group Call (US morning)

Summary:

- Work updates
- Aries crypto service RFC

Note: This call is Recorded. Recordings posted at the bottom of the page.

Date

20 Nov 2019 (7AM Los Angeles, 10AM New York, 3PM London, 18H Moscow)

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 (Employer) <email>**
  - Troy Ronda (SecureKey) <troy.ronda@securekey.com>
  - Stephen Curran (CloudCompass/BC Gov) <swcurran@cloudcompass.ca>
  - Marvin Berstecher (esatus AG) <m.berstecher@esatus.com>
  - Sam Curren (Sovrin Foundation) <sam@sovrin.org>
  - Ajay Jadhav (AyanWorks) <ajay@ayanworks.com>
  - Ken Ebert (Sovrin Foundation) <ken@sovrin.org>
  - Robert Mitwicki
  - Mike Lodder (Sovrin Foundation) <mike@sovrin.org>
  - Richard Esplin (Evernym) <richard.esplin@evernym.com>
  - Wolfgang Lamot (difacturo GmbH) <wolfgang.lamot@difacturo.com>
  - @kamlesh Nagware (Snapper Future Tech) <kamlesh.nagware@snapperfuturetech.com>
  - Bernardus Kurnia (Bina Nusantara University) <michael.bernardus@gmail.com>

Welcome / Introductions

Announcements

- Aries Workshop/Connectathon December 3-5 in Provo, Utah - Dates Confirmed, Food Sponsors welcome!
- Webinar on peer DIDs Nov 21 at 1 PM MST, ssimeetup.org
- Hyperledger edX course launched this week - Introduction to Hyperledger Sovereign Identity Blockchain Solutions: Indy, Aries & Ursa

Related Calls

- Previous Aries Working Group calls
- Identity Implementors Working Group call
  - Main place to get project updates, release status, and announcements.

Release Status and Work Updates

- Aries Protocol Test Suite
  - Progress in making it work with the LibVCX Dummy Cloud Agent (support for mediators).
  - Ready for people to contribute additional tests.
- 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
- Aries-Framework-Go (Troy) Aries-go
  - Working on mediator/routing, WebSocket transport, WASM, browser primitives, credential issuance.
  - Mentioned last week on the B call
    - 0.1.0 released (mentioned last week on the B call).
    - Project description posted in README.
    - You can play with the framework by running BDD tests or with the OpenAPI (swagger) interface.
    - Next up: credential issuance (and continuing with W3C verifiable credentials), WebAssembly & WebSockets.
- Aries-SDK-Ruby (Jack)
  - Updated to 0.0.6 at RubyGems https://rubygems.org/gems/aries-sdk-ruby
  - Rails sample project using aries-sdk-ruby at https://github.com/johncallahan/aries-rails
- Aries-Framework-DotNet (Tomislav)
- Aries-StaticAgent-Python - Now up to 0.6.1; more details
- Aries-Toolbox
  - Moving repos to HyperLedger's Github Org.
  - ACApy plugin for supported admin protocols.
- Aries-SDK-Python - Wrapper from JeromK and SBCA?
- Aries-SDK-Java
- 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
  - Need to rename existing repo - "aries-framework-javascript" to "aries-sdk-javascript" and create a new repo as "aries-framework-javascript"
  - Also need to add following people as maintainers to both repos.
    - Jakub Koci, Matt Raffel, Ajay Jadhav, Keith Smith
  - Regular weekly zoom calls to be scheduled from this Friday. Will share the details on Rocket Chat.
  - DIF people interested in implementing a JavaScript 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

**RFC Progress**

- Rich Schema RFC headed to an APPROVED status, Troy had some comments on how the Link Secrets tie to W3C spec.
- Proposal to renumber RFC 0289

**Other Business**

- Crypto Service RFC, Robert Mitwicki
  - Expose cryptographic services outside of the Agent (e.g. make available for document transfer services).
  - https://github.com/mitfik/aries-rfcs/tree/master/features/0312-crypto-service
  - Next steps with the RFC:
    - Need to address overlap with Aries-KMS.
    - Need to address key exposure post-compromise.
    - Leverage message blinding. (Mike L can help)
    - Include more use cases
      - more specific details (PDF viewer . . . )
      - concern that the process is driven outside the agent, instead of by the agent
      - explain when the compromises in trust-shifting makes sense
      - where is this useful, and where is this not recommended
  - Progress on POCs for Core Libraries: Aries-KMS, Aries-VDRI

**Future Topics**

- Next call
Progress on the Aries Protocol Test Suite
- Hubs vs Agents

Other:
- Status and future of wallet query language
- IoT best practices (Robert Mitwicki, Adam Burdett, Lohan Spies)
- DID Resolution W3C and Sam’s concerns: [https://github.com/hyperledger/aries-rfcs/issues/130](https://github.com/hyperledger/aries-rfcs/issues/130)
- Architecture of Aries Verifiable Credentials Proof Formats (Mike Lodder)

Action items

Call Recording

<table>
<thead>
<tr>
<th>File</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multimedia File GMT20191120-150306_Community_-1920x1440.mp4</td>
<td>Nov 20, 2019 by Richard Esplin</td>
</tr>
</tbody>
</table>