2019-10-30-B Aries Working Group Call (US afternoon)

Summary:

- Review open tickets; which can be resolved? (15 min - Stephen C)
- Signed attachments, -sig, etc (15 min - Kyle, Troy)
- Delegatable creds and consent receipts (30 min - George A, Jan L)
- Cutting over to didcomm.org (15 min - Daniel H)
- Open Discussion / Next Week Topics

Note: This call is being recorded.

Date
30 Oct 2019 (12PM Los Angeles, 3PM New York, Tuesday at 5AM 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](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/BC Gov) <swcurran@cloudcompass.ca>
- George Aristy (SecureKey) <george.aristy@securekey.com>
- John Callahan (Veridium) <jcallahan@veridiumid.com>
- Javier Ochoa (SOMA) <javier@soma.co>
- Troy Ronda (SecureKey) <troy.ronda@securekey.com>
- Ajay Jadhav (AyanWorks) <ajay@ayanworks.com>
- Keith Smith (IBM) <bksmith@us.ibm.com>
- Brent Zundel (Evernym) <brent.zundel@evernym.com>
- Steve McCown (Anonyme Labs) <smccown@anonyme.com>
- Richard Esplin (Evernym) <richard.esplin@evernym.com>
- Paul Knowles (Dativa) <paul.knowles@dativa.com>
- Ken Ebert (Sovrin Foundation) <ken@sovrin.org>
- Tobias Looker (Mattr) <tobias.looker@mattr.global>
- Moushmi Banerjee (Nutanix) <moushmi.banerjee@nutanix.com>
- Cam Parra (Kiva) <camilo@kiva.org>
- Kyle Den Hartog (Mattr) <kyle.denhartog@mattr.global>
- Kaliya "IdentityWoman" Young <kaliya@identitywoman.net>

Welcome / Introductions

Announcements

- Aries Workshop/Connectathon December 3-5 in Provo, Utah - Dates Confirmed, Food Sponsors welcome!
- Please RSVP
- Sovrin Foundation Sovrin Governance Framework GDPR Docs—second public review (15 days) started Oct 23rd—see the links [here](#)
- Other Announcements

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:
- DID UX Call - Stack/Mailing list - details in the shared document as well minutes and additional information, currently bootstrapping discussion about UX for defined personas
- 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 Protocol Test Suite
  - Works, and ready for test contributions
- Aries Core Libraries (agent storage, ledger interface, comms)
  - Planning a move for the Indy Wallet crate into hyperledger/aries-ams
  - Will likely change the name to aries-kms (see vote below)
  - SQLite as the default wallet.
  - aries-ams-sqitle is archived
  - Need to migrate Postgres wallet plugin from Indy to aries-ams-postgres
- Future:
  - Verifiable Data Registry Interface library
  - Static Peer DIDs in aries-vdri as the default implementation
  - aries-vdri-peer is archived
- Aries-CloudAgent-Python (bc.gov) - Release 0.3.5 Coming Soon - mainly cache handling updates.
  - Continuing to learn about performance/storage impacts of using Aries protocols and non-secrets (metadata) interface.
  - Lessons learned:
    - Database calls are fast, but there are a lot of calls being made - take great care in using tags (credentials and protocol state)
    - Protocol state is large - leave it to controller to decide what to keep
    - Really hard to understand inside the KMS - what's happening and getting metrics out.
    - Caching is hard - self-inflicted wound
    - Current issue - not understanding all the calls to "SELECT item" from secrets storage.
- Aries-Framework-Go (Troy)
  - Weekly planning notes (2019-10-29)
  - Closing the 0.1.0 milestone this week.
    - Framework structure.
    - Draft DID Exchange Protocol (including Go and REST "controller" APIs).
    - HTTP Binding for DID resolver along with first phase of peer DID support.
    - Envelope pack/unpack (including support for draft JWE envelopes).
  - Shifting focus to the 0.1.1 milestone.
    - Introduce and issue credential protocols (and finalize DID Exchange).
    - WebSocket transports.
    - Refactor pluggable interface categories (kms, crypto, ...).
    - Stretch goals (in planning page).
- Aries-SDK-Ruby (Jack)
  - Project is featured on Ruby-Flow (http://www.rubyflow.com/p/0fdgjy-ruby-sdk-for-hyperledger-aries)
  - 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) Transaction Authors/Endorser support for Indy.
- Aries-SDK-Python - PR from JeromeK
- Aries-SDK-Java - Usually Wed Evenings
  - Javier => asking help to move forward. Any agenda on what is being developed on other SDKs?
- Aries-SDK-JavaScript - Contributors are now meeting on every Fridays -
  - Need to create a new repo - "aries-framework-javascript" and add following contributors to get started.
    - Jakub Koci, Matt Raffel, Ajay Jadhav, Keith Smith
  - Meeting details are here - Framework JS Meetings
  - See current plan here - FAQs
- Indy
  - Migrating from Indy SDK
  - Closing PRs related to Indy wrappers with pointers to Aries language libraries
  - Adding LibVCX support for some Aries protocols
    - Trouble when testing with ACA-Py as an issuer.
      - https://github.com/hyperledger/aries-cloudagent-python/pull/239
      - https://github.com/hyperledger/aries-cloudagent-python/pull/240
      - https://github.com/hyperledger/aries-cloudagent-python/pull/241
    - Conversations about RFCs versus working implementations.
- Ursa

Agenda

- Review open tickets; which can be resolved? (15 min - Stephen C)
- Signed attachments, ~sig, etc (15 min - Kyle, Troy) discussion for this is happening on Pull request #267 https://github.com/hyperledger/aries-rfcs/pull/267
- Delegatable creds and consent receipts (30 min - George A, Jan L)
- Cutting over to didcomm.org (15 min - Daniel H)
- Not covered: Socialize test suite RFC (5 min - Daniel H)
- Open Discussion / Next Week Topics

Next Week

Future Topics

- Link handling to open Mobile Agents
- 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
• 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

• Aries Working Group B 20191030 Recording
• Aries Working Group B 20191030 Chat