2019-11-06-A Aries Working Group Call (US morning)

Summary:
- Work updates
- Payments in Aries
- Hardware enclaves

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

Date
06 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

- Troy Ronda (SecureKey) <troy.ronda@securekey.com>
- John "Jack" Callahan (Veridium) <jcallahan@veridiumid.com>
- Matt Raffel (Kiva) <mattr@kiva.org>
- Ken Ebert (Sovrin Foundation) <ken@sovrin.org>
- Stephen Curran (Cloud Compass/BC Gov) <swcurran@cloudcompass.ca>
- Richard Esplin (Evernym) <richard.esplin@evernym.com>
- Sam Curren (Sovrin Foundation) <sam@sovrin.org>
- Cam Parra (Kiva) <camilop@kiva.org>
- Steve McCown (Anonyome Labs) <smccown@anonyome.com>
- Brent Zundel (Evernym) <brent.zundel@evernym.com>
- Oskar van Deventer (TNO) <oskar.vandeventer@tno.nl>

Welcome / Introductions

Announcements

- Aries Workshop/Connectathon December 3-5 in Provo, Utah - Dates Confirmed, Food Sponsors welcome!
  - Please RSVP
- Webinar on peer DIDs Nov 21 at 1 PM MST, ssimeetup.org
- Proposal to renumber RFC 0289

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
  - Works, and ready for test contributions
- 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)
  - SQLite as the default wallet.
  - aries-ams-sqlite is archived
• Need to migrate Postgres wallet plugin from Indy to aries-ams-postgres
  • Verifiable Data Registry Interface library
    • Static Peer DIDs in aries-vdri as the default implementation
    • aries-vdri-peer is archived
  • Ken's POC
  • Other Core Libraries (pack / unpack)
  • Aries-CloudAgent-Python (bc.gov) - Release 0.3.5 has been tagged and is on PyPi - caching/performance issues
  • Aries-Framework-Go (Troy)
    • Weekly planning notes (2019-11-05)
    • Wrapping up 0.1.0 release and starting on 0.1.1.
    • https://didcomm.org is now used as the prefix for message types (replaces did:sov:.....)
    • Successful experimentation on the possibility of exposing additional bindings (C, WASM).
      • (We currently have Go and REST.)
    • You can play with the framework by running BDD tests (make bdd-test) or with the OpenAPI (swagger) interface (See README).
  • Aries-SDK-Ruby (Jack)
    • Updated to 0.0.6 at RubyGems https://rubygems.org/gems/aries-sdk-ruby
  • Aries-Framework-DotNet (Tomislav)
  • Aries-StaticAgent-Python
  • Aries-SDK-Python - Wrapper from JeromK and SBCA?
  • Aries-SDK-Java
  • Aries-SDK-JavaScript
    • 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 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 in progress
  • Migration from LibIndy
    • Closing PRs related to Indy wrappers with pointers to Aries language libraries
    • LibVCX support for some Aries protocols
  • Ursa 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

RFQ Progress
• Rich Schema RFC headed to an APPROVED status, Troy had some comments on how the Link Secrets tie to W3C spec.
• New RFC: Trust-over IP Overview RFC 0289
  • https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack
  • RFC 1?
  • Troy’s feedback: https://github.com/hyperledger/aries-rfcs/issues/292
• Proposal for an “RFC 2”
  • Sergey thinks we need an overview of how the many protocols fit together.

Other Business
• Payments in Aries
  • Currently have the payment decorator defines how to request payment and prove that payment happened (same information as the W3C Web Payments standard).
  • Protocol gap in actually making the payment. Should be pluggable (application agnostic).
  • Payments are defined as part of credential issuance and presentation
  • Top level concept like KMS?
• Using hardware enclaves (Mike L.)
  • Agent KMS Considerations:
    • Steve M. has played a lot with the Apple enclave and can help.
    • Tension between security of a hardware enclave, and the portability promises of SSI.
      • Assumption is that any key put into an enclave cannot come out.
    • Ursa will provide an interface for interacting with an enclave (abstract the complexity).
      • Needs flexibility: mobile enclave, enterprise HSM

Future Topics
• Next call
  • Hubs vs Agents
  • Progress on POCs for Core Libraries: Aries-KMS, Aries-VDRI
• 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
  • 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 GMT20191106-150141_Community_-1652x1080.mp4 Call recording</td>
<td>Nov 06, 2019 by Richard Esplin</td>
</tr>
</tbody>
</table>