2019-09-25-A Aries Working Group Call (US morning)

Summary:

- Project update
- Naming of core Aries components
- Plan for Aries "wallet storage"

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

Date
25 Sep 2019 (7AM Los Angeles, 10AM New York, 3PM London, 17H 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 (organization) <email>
- Daniel Bluhm (Sovrin Foundation) <daniel.bluhm@sovrin.org>
- Matt Raffel (kiva) <mattr@kiva.org>
- Ajay Jadhav (AyanWorks) <ajay@ayanworks.com>
- Richard Esplin (Evernym) <richard.esplin@evernym.com>
- Troy Ronda (SecureKey) <troy.ronda@securekey.com>
- Steve McCown (Anonyome Labs) <smccown@anonyome.com>
- Carl DiClementi (Factom Inc) <carl@factom.com>
- Kumaravel N (Ford) <nikumarav2@ford.com>
- Brent Zundel (Evernym) <brent.zundel@evernym.com>
- Cam Parra (Kiva) <camilop@kiva.org>

Welcome / Introductions

Announcements

- Internet Identity Workshop
- Hyperledger Maintainers Summit: Minneapolis October 8-10
- Bootcamp Russia: Event Location
- Aries Workshop/Connectathon December 3-5 in Provo, Utah (details to follow)

Summary of Prior Calls and Related Meetings

- DID WG
  - first meeting last week, good participation. Starting with the existing spec. Hope to be at feature freeze by next spring.
  - DID WG page: https://www.w3.org/2019/did-wg/
  - DID WG did spec repo (feel free to raise issues): https://github.com/w3c/did-spec

- Aries WG
- Indy
- Ursa
  - Question for the Indy team on testing and deploying debian packages

Release Status

- Aries-CloudAgent-Python (bc.gov) - Release 0.3.2 has been tagged and is on PyPi
  - Support for RFC 0036 and RFC 0037 Credential Exchange protocols, 0.1 version of those protocols deprecated
  - Working on next release, particularly on revocation support.

- Aries-Framework-Go (Troy)
  - First milestone: Framework Go v0.1.0
Weekly planning notes (2019-09-24)

- **Aries-SDK-Ruby (Jack)**
  - Released as a Gem (0.0.3) due to Rails 6 issues
  - Developed docker image with Rails 6 (Ruby 2.5.1) with Indy-SDK to test Aries-SDK-Ruby via Dokku deployment
  - Needed for exploring concurrency and compatibility issues with Sidekiq, Resque, SuckerPunch, etc.

- **Aries-Framework-DotNet (Tomislav)**
  - Moved from StreetCred to Aries: https://github.com/hyperledger/aries-framework-dotnet

- **Aries-StaticAgent-Python**
  - Move from PySodium to PyNacl
  - Improved module interface and routing.

- **Aries-SDK-Java**
  - Aries-SDK subchannel / discussion aries-sdk-java

- **Aries-SDK-JavaScript**
  - https://github.com/hyperledger/aries-sdk-javascript/pulls
  - Starting to implement the Aries RFCs.

- **Indy**
  - Working on release of 0.2.0 (September / October)
    - ZKP / ZKLang improvements
    - Debian packages
    - Refactor internal plumbing for anoncreds 2.0, shouldn't impact external interfaces
    - Refactor multi-signature BLS in addition to aggregated signature
    - Sovrin Foundation is looking to build a Indy specific Ursa, with ZKP. Other Aries clients would build a different Ursa.

**Work Updates**

- **Rich Schemas and W3C Verifiable Credentials (Ken)**
  - Working on context object in Node. PR for Indy-Node is almost ready for review.
  - Making progress on the new schema object.
  - In order to do the review, need new Indy HIPes: each new object, the new flow for creating credentials, creation of presentation request and presentation, compatibility with the old credential format

- **SDK 2.0 architecture / Indy-Aries split (Sergey)**
  - http://jira.hyperledger.org/browse/IS-1285
  - https://docs.google.com/document/d/1MYM6i4NkxoJoC79WBOIX_QA3_9rG-iK3iZa86vIR0/edit#heading=h.z1u0dzf62oi POA and discussion
  - https://docs.google.com/drawings/d/1d-aCRC_Nzyyw9nyQi9_vBGbeWhp69M4T5_8_yYTAl/edit?usp=sharing Indy SDK Migration box diagram
  - https://docs.google.com/drawings/d/1stUlfkRPlufingeeRjibNvI9Ek3CNi9h9IQym8mU4M/edit?usp=sharing Aries Architecture
  - https://hackmd.io/_BhJewTlSUqMGNDc4SvgNw?edit# developing ideas around APIs
  - Aries Presentations
  - https://hackmd.io/@gjPgYQjMT3azdpSAFgo5PA/HylVdhVGr Daniel B's proposal for separating wallet and crypto
  - https://docs.google.com/document/d/18kHgTslShkSlIw9cabmpv8rxKxNchWycbHnXGyxts/edit# developing ideas around APIs

- **Architecture of Aries Verifiable Credentials Proof Formats**
  - Boundary between the claim type and the signature type
  - Where should it live? Anoncreds (ZKP), JWTs, Link Data Signatures

- **RFC Progress**

- **Other Business**

- **Kiva and plan for aries-wallet**
  - W3C DID compliant storage library (discussion at RWOT, but no standard today)
  - More testing
  - Contributor diversity
  - Wallet mobile support

- **Architecture of Aries core library**
  - What is our fastest path to a library that framework implementors could consider using?

- **Naming**
  - aries-wallet aries-ams (agent managed storage)
  - aries-wallet-postgres aries-ams-postgresql
  - aries-wallet-sqlite aries-ams-sqlite
  - aries-resolver-peer and aries-resolver-indy

- **Future Topics**
• Next call
• Other:
  • Hubs vs Agents
  • Payments in Aries
  • 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

Action items

Call Recording

<table>
<thead>
<tr>
<th>File</th>
<th>Modified</th>
<th>Modified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multimedia File GMT20190925-140217_Community-_1494x1080.mp4</td>
<td>Sep 25, 2019</td>
<td>Richard Esplin</td>
</tr>
</tbody>
</table>