2020-06-03-B Aries Working Group Call (US afternoon)

Summary:

- Issue Game: Can we close this?
- OOB For Invitations
- Web site Auth (SIOP?)
- Aries Import/Export

Note: This call is being recorded.

Date

03 Jun 2020 (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

- Sam Curren (Indicio) <sam@indicio.tech>
- George Aristy (SecureKey) <george.aristy@securekey.com>
- Stephen Curran (Cloud Compass Computing Inc.) <swcurran@cloudcompass.ca>
- Steve McCown (Anonyome Labs) <smccown@anonyome.com>
- @Keith Smith (IBM) <bksmith@us.ibm.com>
- Drummond Reed (Evernym) <drummond.reed@evernym.com>

Welcome / Introductions

Announcements

Related Meetings Review

- Ursa -
- Semantics - Next meeting: Never - transitioning to be in the ToIP Foundation - see RocketChat channel for details and how to join the successor group
- DID UX Call - Active?
- SSI in IoT WG
- Identity WG / Identity WG Implementer calls (Wed / Thurs)
- DIF DIDComm WG - Monday's at Noon US/Pacific - Sam Curren (Mon) - DID Doc services, etc.

Upcoming Releases and Work Updates

- Aries Protocol Test Suite
  - One agent under test
  - Issue, credential, and proof tests are merged.
- Aries Agent Test Harness
  - Test compatibility between any two agents
  - Real Soon Now: Bounty for implementing the Aries Framework .NET backchannel (and maybe others)
  - https://github.com/bcgov/aries-agent-test-harness
- Aries Shared:
  - Aries Shared:
    - indy-vdr (Andrew Whitehead) https://github.com/hyperledger/indy-vdr
    - Nearing release 0.6(?) - most work complete that was needed: Design doc, FFI, testing, CI / CD
    - CI - GitHub actions run unit tests and basic integration tests
    - CD not there
    - No design doc, but crate docs
Rich Schema merged and behind a feature flag
Refactoring PR not merged - cleanup, internal simplification, crate docs

- indy-credx - https://github.com/bcgov/indy-credx
  - Experimental ACA-Py branch created that can do credential exchange with indy-credx
- indy-shared-rs - https://github.com/bcgov/indy-shared-rs
  - Shared features across indy-vdr and indy-credx
  - pack/unpack on Ursa (not libsodium)
- aries-credx
  - https://github.com/sovrin-foundation/aries-credx-framework-rs
  - 6 most common attribute encodings (but not anoncreds 1 attribute encoding)
  - Can make a non-revocable credential and create proofs.
- Aries Secure Storage initiatives:
  - Mike working on documentation and architecture as an Aries RFC (KMS architecture) and Ursa RFC (API)
  - PR is submitted: https://github.com/hyperledger/aries-rfcs/pull/440
  - Mike and Cam's work aries-kms-mayaguez - Postgres backend for credential storage
    https://github.com/sovrin-foundation/aries-kms-rs
  - Persistence work allows plugging in any database engine.
  - Focus is using an external enclave.
  - aries-kms-vostok - indy-wallet capabilities moved to an Aries base
  - Andrew also working on that

- Aries-CloudAgent-Python (bc.gov)
  - Release 0.5.1 is on PyPi:
  - Revocation support added and tested with Streetcred and esatus Mobile Agents; major/minor version handling
- Aries-Framework-Go (Troy) #aries-go
  - Implementing the Out-Of-Band protocol
  - Implementing issue-credential and present-proof protocols
  - Edge agent in work based aries-framework-go using WASM with support for DID, VCs and DIDComm support being added
- Aries-SDK-Ruby (Jack)
  - Added DID/Verkey sign_and_submit to aries-sdk-ruby and published new gem (0.0.8)
  - Created aries-rails-docker experiment that support Rails 4 with Indy 1.8.1 on Heroku & Dokku
- Aries-Framework-DotNet (Tomislav)
  - Release last week for Aries compatibility with ACApy and LibVCX (RFC 0094)
- Aries-StaticAgent-Python
- Aries-Toolbox
  - PR for Connections Update
  - Converted to a web application by Robert Mitwicki : repo https://github.com/thclab/aries
  - Upcoming cleanup items
- Aries-SDK-Java
- Aries-Framework-JavaScript
  - Started regular meetings: Framework JS Meetings
  - Current focus is on mediator use case (NodeJS)
- Rich Schemas and W3C Verifiable Credentials (Brent & Ken)
  - Some work has been done to support the W3C Verifiable Credentials Data Model specification
- Aries-MobileAgent-Xamarin (Aries MAX)
  - Evolution of the open source mobile agent (Mattr Global's OSM Ascend)
    https://github.com/hyperledger/aries-mobileagent-xamarin
- Ursa
  - 0.4.0 scheduled for late March
    - Improved hash to curve algorithm
    - Updates to AMCL wrapper
    - To replace libsodium, need to have a replacement for the anoncrypt / authcrypt sealed box for pack / unpack.
      - Can be done in Ursa with two steps, but might add as a single function call.
    - Revocation 2.0 Support - new approach: Non-Revocation Range Merkle Tree - Ursa RFC here
      - Performance looks good at 1M creds/registry - 16M might be possible.

Agenda

- Intro and project updates (10 min - )
- Issue Game: Can we close this? (15 min - )
  - PR 437 - Service Decorator Requirements for Multi-message Protocols
  - PR 452 - Remove Redundant State
  - PR 482 - Coprotocols
  - PR 486 - Present Proof v2
- OOB Community Support (Stephen Curran) - Presentation
- Web Auth Community Poll (SIOP?) (Sam Curren)
  - DID spec just became clear enough to make this happen.
  - Authentication Section of DID Doc
  - Not a fan of 'prove to id provider'
  - WebAuthn / OIDC - mostly bound to identity provider
  - Symmetry important (user challenge website, etc)
  - Manifold - PicoLabs
- Aries Import/Export Minimum Requirements (Sam Curren)
- Open Discussion / Next Week Topics / Wrap Up (5 min - )

Next Week

- Requests?
Future Topics

- Migrating to new JWE envelope format: [https://github.com/hyperledger/aries-rfcs/issues/478](https://github.com/hyperledger/aries-rfcs/issues/478)
- DIF Interop Project - Project is proceeding, connect the communities at IIW
- DKMS status
- Credential Fraud: Example how in ACA-Py to verify same link secret across multiple credentials in presentation
- Schema interop - how to reused schema across different networks [Robert Mitwicki](https://github.com/hyperledger/aries-rfcs/pull/366) (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](https://github.com/hyperledger/aries-rfcs/pull/366)
- Formal protocol verification techniques - Presented in the Aries WG A Call - 2020.04.08 call
  - [https://github.com/johncallahan/needham_shroeder_spin](https://github.com/johncallahan/needham_shroeder_spin) (non-Aries example using SPIN/Promela)
- What's left for DID Exchange protocol?
  - Some discussion in: [https://github.com/hyperledger/aries-rfcs/pull/366](https://github.com/hyperledger/aries-rfcs/pull/366)

Action items

Call Recording

<table>
<thead>
<tr>
<th>File</th>
<th>Modified</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>