2020-02-05-B Aries Working Group Call (US afternoon)

Summary:

Planned:

- RFC Game: Can we merge this?
- Protocol Semver
- Endpointless agents
- DID Exchange
- Named states and coprotocols

Note: This call is being recorded.

Date

05 Feb 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

- Name (Organization) <email>
- Stephen Curran (Cloud Compass/BC Gov) <swcurran@cloudcompass.ca>
- Richard Esplin (Evernym) <richard.esplin@evernym.com>
- Alexis Falquier (Spaceman ID) <alexis@spaceman.id>
- John Callahan (Veridium) <jcallahan@veridiumid.com>
- George Aristy (SecureKey) <george.aristy@securekey.com>
- Steve McCown (Anonyome Labs) <smccown@anonyome.com>
- Daniel Hardman (Evernym) <daniel.hardman@evernym.com>

Welcome / Introductions

Announcements

- Hyperledger Diversity, Civility, and Inclusivity Survey

Related Meetings Review

- Ursa - No calls since the last Aries meeting.
- Semantics - yesterday's call: Handling big data in an Indy Credential - workaround - Hashlink. Link to Paper
- DID UX Call - Slack/Mailing list - details in the shared document as well minutes and additional information, currently focus on Purpose Based Services
    - F2F Meeting meetup
- SSI in IoT WG
- Indy Contributors - Richard Esplin (Mon) - Notes
- Identity WG / Identity WG Implementer calls (Wed / Thurs) - no calls since last Aries meeting
- DIF DIDComm WG - Monday's at Noon US/Pacific
- W3C DID Working Group F2F meeting in Amsterdam (Jan 29-31)
    - Slides from the F2F meeting (200+)
    - SSI Meetup Webinar by Drummond Reed & Markus Sabadello with a full recap of the F2F meeting

Upcoming Releases and Work Updates

- Aries Protocol Test Suite
    - Thanks again to Keith Smith, Issue Credential tests are merged; Present Proof soon to follow once some minor merge conflicts are resolved.

- Aries Shared:
  - Aries KMS
  - Verifiable Data Registry Interface (VDRI) library: indy-vdr (Andrew Whitehead) https://github.com/andrewwhitehead/indy-vdr
  - Other Core Libraries (pack / unpack)
- Aries-CloudAgent-Python (bc.gov) - Release 0.4.1 is released, with a change to the forward message handling for compatibility with RFC.
  - Release 0.4.2 coming soon with a regression fix related to the ephemeral challenge.
  - Deployment of 0.4.1 to be synchronized to the Streetcred Agent release, which estimated to be in the next couple of days.
  - ACA-Pug (User Group) starting, with first meeting next Wednesday, 1 hour before this meeting. ACA-Pug page is here.
- Aries-Framework-Go (Troy) #aries-go
  - Released v0.1.1
  - Route coordination and forwarding implemented (RFC 94 and RFC 211) and integrated with DID Exchange. Go API Package | BDD test
    - Question raised on how to reconcile RFC 94 and RFC 211.
  - Basic JavaScript scaffolding implemented for browser and node.js to use the WASM. NPM packaging in progress.
    - Next: expose framework operations (similar to the REST API).
  - External message handler and purpose decorator implemented (RFC 351). REST API in progress.
  - HTTP over DIDComm in progress (RFC 335). HTTP request portion implemented.
  - Continuing efforts on routing & relays, crypto/kms, WebAssembly, verifiable credentials, generic message handlers (and external registration), JWE envelopes.
- Aries-SDK-Ruby (Jack)
- Aries-Framework-DotNet (Tomislav)
- Aries-StaticAgent-Python - Now up to 0.6.1; more details
- Aries-Toolbox
  - Official repo moved to aries-toolbox
  - Preparing for a new release based on the latest ACA-Py
- Aries-SDK-Python - Wrapper from JeromK and SBCA?
- Aries-SDK-Java
- Aries-Framework-JavaScript / Aries-SDK-JavaScript
  - As agreed in the connect-a-thon, planning efforts on merging the **aries-sdk-javascript** codebase into a single framework repo - **aries-framework-javascript**
  - Starting with the efforts on the React-Native Mobile Agent.
- 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
- Ursa 0.3.1 release in January
  - Delegate-able credentials
  - Flexible configuration options
  - ZMix 0.1.0 expected in January
    - Ursa and ZMix will be separate releases. ZMix is the proving code, and Ursa is everything else.

Agenda

- ~~Issue~~ PR Game: Can we merge this? (15 min):
- Protocol Semver
  - Additional data in protocol needs a version bump?
  - need template update per 0003
- Service Block / Endpoint URI for Agents without an endpoint (Issue 405)
  - Needs to know which key to encrypt for.
  - The implication is that agent will 'pick-up' messages
- DID Exchange (RFC)
  - Extraction of Invitation Protocol? - Yes (Sam if nobody beats me to it.)
    - note about security
    - includes inline keys described below
    - use of ~service decorator
      - inline key representations - use did:key: as a temporary solution
    - reference of 0268 Deep Linking RFC
    - solve reuse problem by starting a protocol
  - pass DID Docs as attachments
    - replace inline ~sig with attachment signatures
- Named states and coprotocols Daniel Hardman
- Chained Credentials RFC 104 - Paul/Jan
- Open Discussion / Next Week Topics

Next Week

Future Topics

- 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(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
- Formal protocol verification techniques
    - https://github.com/SvenHammann90/SSI/blob/master/RWOT_9/Topic_Paper_RWOT.md (using Tamarin)
    - 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

Action items

Call Recording

File	Modified
Multimedia File GMT20200205-200341_Aries-WG-C_1934x2104.mp4	Feb 10, 2020 by Sam Curren
Multimedia File GMT20200205-200341_Aries-WG-C.m4a	Feb 10, 2020 by Sam Curren
Text File GMT20200205-200341_Aries-WG-C.txt	Feb 10, 2020 by Sam Curren

Download All