2020-01-15-B Aries Working Group Call (US afternoon)

Summary:

- Issue Game: Can we close this?
- Generic JSON Protocol
- ~service decorator
- Connection Blues contined.

Note: This call is being recorded.

Date

15 Jan 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>
- George Aristy (SecureKey) <george.aristy@securekey.com>
- Filip Burlacu (SecureKey) <filip.burlacu@securekey.com>
- Sam Curren (Sovrin Foundation) <sam@sovrin.org>
- Stephen Curran (BC Gov/Cloud Compass) <swcurran@cloudcompass.ca>
- Tobias Looker (Mattr) <tobias.looker@mattr.global>
- Drummond Reed (Evernym) <drummond.reed@evernym.com>
- Daniel Bluhm (Sovrin Foundation) <daniel.bluhm@sovrin.org>
- Steve McCown (Anonyome Labs) <smccown@anonyome.com)
- Moushmi Banerjee (Nutanix) <moushmi.banerjee@nutanix.com>

Welcome / Introductions

Announcements

- Updated Hyperledger Calendar: Calendar of Public Meetings
- Aries-6 Community Confirmation: Move BC Gov Credential Registry contribution "Indy Catalyst" to Aries, calling it "aries-verifiable-credential-registry" (Aries VCR)

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
- SSI in IoT WG
- Indy Contributors - Richard Esplin (Mon) - No call this week
- Identity WG / Identity WG Implementer calls (Wed / Thurs) - no calls since last Aries meeting
- DIF DIDComm WG - Monday's at Noon US/Pacific

Upcoming Releases and Work Updates

- Aries Protocol Test Suite
  - Feature Discovery protocol tests now in test suite thanks to the efforts of Keith Smith
  - Moving on to Issue Credential; first targeting Indy ledger specific tests with the hope of informing design of ledger agnostic tests.
- Aries Shared:
  - Aries KMS
  - Verifiable Data Registry Interface (VDRI) library

- - - Other Core Libraries (pack / unpack)
  - Aries-CloudAgent-Python (bc.gov) - Latest is Release 0.4.0 on PyPi. Some small updates. Big contribution of a set of three sample controllers using different tech stacks.
    - 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
    - 2020-01-14 Framework Go Weekly Planning
    - RFC implementation status and Wishlist (Dec/2019)
    - Continuing efforts on routing & relays, crypto/kms, WebAssembly, verifiable credentials, generic message handlers (and external registration), JWE envelopes.
    - WASM is working for DID Exchange from a browser (running the WASM) to a routing agent. Next we want to show DID Exchange between browsers.
    - Working on design for JS Worker interface for Aries Framework Go WASM.
  - 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
  - Migration from LibIndy
    - Additional LibVCX Aries protocol support released in December.
  - 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 Game: Can we close this? (15 min -) - Stephen Curran issues (as time permits): #336, #201, #334, #317, #114 - Presentation
  - Decisions
    - 336 - close
    - 201 - close
    - 334 - Troy Ronda to update RFC and close
    - 317 - Daniel Bluhmto review and recommend changes
    - 114 - Daniel Hardmandid PR and closed as we talked (thanks!).
- Purpose Decorator (RFC 351) and HTTP over DIDComm (RFC 335) - Filip Burlacu
- Should the ~service decorator be part of AIP 1.0.0? PR link. Richard Esplin
- Connection Blues - Continued - Sam Curren/ Stephen Curran
- 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 ProVerif)
  - https://github.com/johncallahan/needham_shroeder_spin (non-Aries example using SPIN/Promela)

Action items

Call Recording

File	Modified
Multimedia File GMT20200115-200355_Aries-WG-C.m4a	Jan 16, 2020 by Sam Curren
Text File GMT20200115-200355_Aries-WG-C.txt	Jan 16, 2020 by Sam Curren
Multimedia File GMT20200115-200355_Aries-WG-C_3320x2046.mp4	Jan 16, 2020 by Sam Curren

Download All