2019-11-13-B Aries Working Group Call (US afternoon)

Summary:

- What is Aries?
- Aries Stable RFC
- Open Discussion / Next Week Topics

Note: This call is being recorded.

Date

13 Nov 2019 (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>
- Troy Ronda (SecureKey) <troy.ronda@securekey.com>
- Paul Knowles (Dativa) <paul.knowles@dativa.com>
- George Aristy (SecureKey) <george.aristy@securekey.com>
- Sam Curren (Sovrin Foundation) <sam@sovrin.org>
- John Callahan (Veridium) <jcallahan@veridiumid.com>
- Stephen Curran (Cloud Compass/BC Gov) <swcurran@cloudcompass.ca>
- Daniel Bluhm (Sovrin Foundation) <daniel.bluhm@sovrin.org>
- Ajay Jadhav (AyanWorks) <ajay@ayanworks.com>
- Richard Esplin (Evernym) <richard.esplin@evernym.com>
- Tobias Looker (Mattr) <tobias.looker@mattr.global>
- Mike Lodder (Sovrin) <mike@sovrin.org>
- Darrell O'Donnell (CULedger) <darrell.odonnell@culedger.com>
- Ken Ebert (Sovrin Foundation) <ken@sovrin.org>
- Robert Mitwicki The Human Colossus Lab
- Alain Neyroud IBM <neyroud@us.ibm.com>
- Moushmi Banerjee Nutanix <moushmi.banerjee@nutanix.com>

Welcome / Introductions

Announcements

- Aries Workshop/Connectathon December 3-5 in Provo, Utah
  - Thank you Sponsors: StreetCred and Hyperledger! - More Food Sponsors welcome!
  - Please RSVP
- Webinar on peer DIDs Nov 21 at 1 PM MST, ssimeetup.org

Related Meetings Review

- Ursa - Progress on packages and Plenum work.
- Semantics - ODCA pilots underway - The agenda, video, notes, etc. from the **HL Indy Semantics WG** call:

Unknown macro: 'lref-gdrive-file'

  - Read more: https://odca.online and https://tool.odca.online
  - Fully functional parser: https://github.com/THCLab/odca-ruby
- 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) - Discussed future of Indy Ledger (View Change, Aardvark BFT, bug fixes, future of Plenum)

- Identity WG / Identity WG Implementer calls (Wed / Thurs)

Upcoming Releases and Work Updates

- Aries Protocol Test Suite
  - Works, and ready for test contributions
- Aries Core Libraries (agent storage, ledger interface, comms)
  - Planning a move for the Indy Wallet crate into hyperledger/aries-kms
    - SQLite as the default KMS plugin.
    - aries-kms-sqlite is archived
  - Need to migrate Postgres capability to aries-kms-postgres
  - Future:
    - Verifiable Data Registry Interface library
    - Static Peer DIDs in aries-vdri as the default implementation
    - aries-vdri-peer is archived
- Aries-CloudAgent-Python (bc.gov) - current Release 0.3.5. Continued instrumentation, performance learning
  - OrgBook transaction rate now at 50% of VON-X version - a significant improvement. Instrumentation is huge!!
- Aries-Framework-Go (Troy) #aries-go
  - 0.1.0 released.
  - Project description posted in README.
  - Weekly planning notes (2019-11-12).
  - You can play with the framework by running BDD tests or with the OpenAPI (swagger) interface.
  - Next up: credential issuance (and continuing with W3C verifiable credentials), WebAssembly & WebSockets.
- Aries-SDK-Ruby (Jack)
  - Project is featured on Ruby-Flow (http://www.rubyflow.com/p/ofdqjq-ruby-sdk-for-hyperledger-aries)
  - Updated to 0.0.6 at RubyGems https://rubygems.org/gems/aries-sdk-ruby
  - Rails sample project using aries-sdk-ruby at https://github.com/johncallahan/aries-rails
- Aries-Framework-DotNet (Tomislav) Transaction Authors/Endorser support for Indy.
- Aries-SDK-Python - PR from JeromeK - weigh-in from those interested in Python wrapper would be appreciated.
- Aries-SDK-Java - Usually Wed Evenings #aries-framework-java
  - Javier => asking help to move forward. Any agenda on what is being developed on other SDKs?
- Aries-SDK-JavaScript - #aries-javascript
  - Contributors are now meeting on every Fridays -
  - PR for moving Indy NodeJS wrapper repo has been merged into https://github.com/hyperledger/aries-framework-javascript
  - Ready for contributors to start picking next tasks
  - Need to create a new repo - "aries-framework-javascript" and add following contributors to get started.
    - Jakub Koci , Matt Raffel , Ajay Jadhav , Keith Smith
  - Meeting details are here - Framework JS Meetings
  - See current plan here - FAQs
  - Bug in Indy-SDK NodeJS wrapper seems relevant to Aries code base: IS-1422
- Indy
  - Plans to immediately deprecate Indy wrappers for Python and DotNet (IS-1423), will do later Java, JavaScript, iOS (IS-1424)
  - Plans to immediately deprecate Indy Documentation / Getting Started Guide in favor of Aries (IS-1425)
  - Undecided about the timing for deprecating LibVCX (IS-1416)
  - Rich Schemas
    - New RFC under review for the schema object (and corresponding HIPE in Indy). https://github.com/hyperledger/aries-rfcs/tree/master/features/0281-rich-schemas
- Ursa
  - 0.3 release by the end of the month.

Agenda

- Issue Game: Can we close this? (15 min)
  - #97 - For non local agents, should HTTPS still be required?
  - #100 - RFC 0019: Are the additional layers of encryption relevant for security or (only) privacy?
  - #101 - DID Resolution work
- What is Aries? (30 min - Sam Curren)
- Aries Stable RFC (20 min - Stephen Curran)
- Open Discussion / Next Week Topics

Next Week

Future Topics

- DIF Interop Project - Project is proceeding, connect the communities at IIW
- DKMS status
- Independent agent upgrades
- Signature Envelope (Kyle)
  - Updating to JWE compliant data model
- Credential Fraud: Example how in ACA-Py to verify same link secret across multiple credentials in presentation
- 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
- Update message type and protocol identifier to https. (and protocol documentation hosting.)
- 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](https://github.com/johncallahan/needham_shroeder_spin))

Action items

Call Recording

File	Modified
Multimedia File GMT20191113-200416_Aries-WG-C.m4a	Nov 14, 2019 by Sam Curren
Text File GMT20191113-200416_Aries-WG-C.txt	Nov 14, 2019 by Sam Curren
Multimedia File GMT20191113-200416_Aries-WG-C_2282x1928.mp4	Nov 14, 2019 by Sam Curren

[Download All](#)