

# 2020-04-15-B Aries Working Group Call (US afternoon)

## Summary:

### Plans

- Issue Game: Can we close this?
- Demo: Immunity Credential
- Revocation 2.0
- DID Exchange / OOB Update

Note: This call is being recorded.

## Date

15 Apr 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>
- Sam Curren (Indicio) <sam@indicio.tech>
- [John Callahan](#) (Veridium) <jcallahan@veridiumid.com>
- [Drummond Reed](#) <drummond.reed@evernym.com>
- [Stephen Curran](#) (Cloud Compass Computing Inc.) <swcurran@cloudcompass.ca>
- [Cam Parra](#) (Kiva) <camilop@kiva.org>
- [George Aristy](#) (SecureKey) <george.aristy@securekey.com>
- [Steve McCown](#) (Anonymo Labs) <smccown@anonymo.com>
- [Paul Knowles](#) (The Human Colossus Foundation) <paul.knowles@humancolossus.org>

## Welcome / Introductions

## Announcements

- [IIW](#) April 28-30 Will happen, in digital form.

## Related Meetings Review

- Ursa -
- Semantics - Next meeting: 04/28 (Tuesday)
- [DID UX Call](#) - Active?
- [SSI in IoT WG](#)
- Indy Contributors - No call this week
- Identity WG / Identity WG Implementer calls (Wed / Thurs) - Riley Hughes on status of Sovrin Mainnet
- DIF DIDComm WG - Monday's at Noon US/Pacific - [Sam Curren](#) (Mon) - Continued discussion of zero round trip (0rtt) vs. Out of Band/DID Exchange connections.

## Upcoming Releases and Work Updates

- Aries Protocol Test Suite - <https://github.com/hyperledger/aries-protocol-test-suite>
- Aries Agent Test Harness - <https://github.com/bcgov/aries-agent-test-harness>
  - A harness for testing two or more agent implementations using RFC-driven BDD test scripts
  - POC evolving into a test harness
  - Help Wanted: Creating a backchannel integration for aries-framework-dotnet
- Aries Shared Components:
  - indy-vdr ([Andrew Whitehead](#)) <https://github.com/hyperledger/indy-vdr>

- Remaining work: Wrap up for a 1.0 release
  - On Hold: Integrating into LibIndy in a separate branch, goal is to release in April/May
- indy-credx ([Andrew Whitehead](https://github.com/andrewwhitehead/indy-credx)) <https://github.com/andrewwhitehead/indy-credx>
- + indy-shared-rs ([Andrew Whitehead](https://github.com/andrewwhitehead/indy-shared-rs)) <https://github.com/andrewwhitehead/indy-shared-rs>
  - Shared code for indy-vdr and indy-credx
  - Currently utils for: ed25519, hash, wql
- aries-credx ([Mike Lodder](https://github.com/sovrin-foundation/aries-credx-framework-rs)) <https://github.com/sovrin-foundation/aries-credx-framework-rs>
  - Currently just claim encoding routines
  - Future TBD
- Aries-KMS/Storage ([Mike Lodder](#) [Andrew Whitehead](#) [Cam Parra](#))
  - [Mike's presentation in Aries WG A](#)
  - Mike and Cam's aries-core-rs aries-kms-mayaguez <https://github.com/sovrin-foundation/aries-kms-rs>
  - aries-kms-vostok: evolution of the Indy wallet crate as a starting point
  - Next steps likely from [Mike Lodder](#) and [Andrew Whitehead](#) - others interested and have time?
- Aries-CloudAgent-Python (BC Gov)
  - 0.5.0 Real Soon Now
  - Revocation based on anoncreds 1.0 has been merged into master and will be in the next release.
    - Successful tests with Streetcred and esatus wallets 😊
  - Signing of Attachments
  - Major/Minor protocol version handling
  - Tracing based on [RFC 0034](#) and trace output visualization. Goal is "jurisdiction-scale" issuance.
- Aries-Framework-Go (Troy) #aries-go
  - Issue credential protocol with [BDD tests](#).
  - Continuing work on out-of-band and present proof protocols.
- Aries-SDK-Ruby (Jack)
  - Trying to resolve dependabot vulnerabilities in ruby gems used by the aries-sdk-ruby and example Rails projects
- Aries-Framework-DotNet (Tomislav)
- Aries-StaticAgent-Python
- Aries-Toolbox
- Aries-SDK-Java
  - Initial PR
- Aries-Framework-JavaScript / Aries-SDK-JavaScript
  - Started regular meetings: [Framework JS Meetings](#)
- Rich Schemas and W3C Verifiable Credentials (Brent & Ken)
- Ursa

## Agenda

- Intro and project updates (10 min - )
- IIW Plans/Demos involving Aries? (10 min - Sam Curren)
  - BCGov - Credential Demos Covid-19 related
    - Integration with mobile wallets etc. (Streetcred, eSatus)
- Immunity Demo (15 min - Jan L)
- Revocation 2.0 (15 min - Stephen Curran) - [Presentation](#)
- DID Exchange / OOB Update (10 min - Sam Curren)
  - OOB Updates
    - <https://github.com/hyperledger/aries-rfcs/pull/454>
    - <https://github.com/hyperledger/aries-rfcs/pull/461>
  - REuse-accepted <https://github.com/hyperledger/aries-rfcs/pull/455>
  - DID Exchange Role Names <https://github.com/hyperledger/aries-rfcs/issues/457>
  - Will this bridge GO/DotNet/ACA-py?
- Common Use Cases Opportunities (5 min - Sam Curren)
- Issue Game: Can we close this? (15 min - )
- Open Discussion / Next Week Topics / Wrap Up (5 min - )

## Next Week

- Requests?

## 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](https://github.com/SvenHammann90/SSI/blob/master/RWOT_9/Topic_Paper_RWOT.md) (using [Tamarin](#))
  - [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>

Action items

Call Recording

File	Modified
Multimedia File GMT20200415-185718_Aries-WG-C_3158x2046.mp4	Apr 21, 2020 by Sam Curren
Multimedia File GMT20200415-185718_Aries-WG-C.m4a	Apr 21, 2020 by Sam Curren
Text File GMT20200415-185718_Aries-WG-C.txt	Apr 21, 2020 by Sam Curren

[Download All](#)