

2019-12-11-B Aries Working Group Call (US afternoon)

Summary:

- please_ack in the issue_credentials protocol
- Connectathon review

Note: This call is being recorded.

Date

11 Dec 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 Updegrave of the firm of Gesmer Updegrave LLP, which provides legal counsel to the Linux Foundation.

Attendees

- Name (Organization) <email>
- Troy Ronda (SecureKey) <troy.ronda@securekey.com>
- Stephen Curran (Cloud Compass/BC Gov) <swcurran@cloudcompass.ca>
- [George Aristy](#) (SecureKey) <george.aristy@securekey.com>
- [Richard Esplin](#) (Evernym) <richard.esplin@evernym.com>
- [Drummond Reed](#) (Evernym & Sovrin Foundation) <drummond.reed@evernym.com>
- [Steve McCown](#) (Anonymo Labs) <smccown@anonymo.com>
- [Paul Knowles](#) (Dativa) <paul.knowles@dativa.com>
- [Sam Curren](#) (Sovrin Foundation) <sam@sovrin.org>

Welcome / Introductions

Announcements

- New Indy/Aries/Ursa edX course, now online - [enroll now!](#)
- Dec 25th and Jan 1st calls canceled for holidays
- DIF Alignment call tomorrow Noon US/Mountain <https://zoom.us/j/466295244>
- Updated Hyperledger Calendar: [Calendar of Public Meetings](#)

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

Upcoming Releases and Work Updates

- Aries Shared Libraries
 - Aries-Shared-KMS
 - BC.gov team will be moving Indy Wallet to Aries-Shared-KMS, Aries-Shared-KMS-PostgreSQL, and Aries-Shared-KMS-SQLite
 - Aries-Shared-VDRVerifiable Data Registry Interface library

- Waiting to finalize the common interface until we have multiple implementations.
 - Starting with Indy-Aries-VDR
 - Aries-Shared-Creds
 - Waiting to finalize the common interface until we have multiple implementations.
 - Starting with Indy-Aries-Anoncreds
 - Aries-Shared-Util
 - Will be moving pack / unpack from LibIndy
- Aries-CloudAgent-Python (bc.gov) - Release 0.4.0 is out on [PyPi](https://pypi.org/). See release notes [here](#).
 - Breaking Change: General refactoring - modules moved from messaging into new core, protocols, and utils sub-packages [#250](#), [#301](#)
 - Existing plugins will be reported as not found, as they need to be moved to use the new structure.
 - Startup parameter `--protocol` changed to `--plugin` to reflect that plugins can be used for other purposes than just adding protocols.
 - Heads up [Daniel Bluhmand](#) [Sam Curren](#) as this may affect deployments of Aries Toolbox.
 - Other noteworthy changes:
 - Replaced v0.1 Credential Exchange with v1.0 everywhere it wasn't being used for demos, etc.
 - Added support for protocols used by the [vc-authn-oidc](#) IdP
 - Improvements based on high volume issuing performance investigation in deploying Indy Catalyst.
- Aries-Framework-Go (Troy) [#aries-go](#)
 - [Weekly planning notes \(2019-12-10\)](#).
 - Successfully performed DID Exchange using a WASM (+ Vue.js) app running in the browser (via WebSockets).
 - Next step: Perform DID Exchange between two WASM apps running in browsers (forwarded via connected mediators). [Diagram](#).
 - Working on mediator/routing, WASM, browser primitives, JWE envelope.
- Aries-SDK-Ruby (Jack)
 - No update this week
- Aries-Framework-DotNet (Tomislav)
- Aries-StaticAgent-Python - [0.7.0](#)
- Aries-Toolbox
- Aries-SDK-Python - Wrapper from JeromK and SBICA?
- Aries-Framework-Java [#aries-framework-java](#) on RocketChat
- Aries-SDK-JavaScript
 - PR for moving Indy NodeJS wrapper repo has been merged into <https://github.com/hyperledger/aries-framework-javascript>
 - Repo is ready for contributors to start picking next tasks
 - Regular weekly zoom calls to be scheduled from this Friday. Will share the details on Rocket Chat.
 - DIF people interested in implementing a Java Script library that might share some of the functionality of the Aries SDK. We need to keep that in mind.
- 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
 - Closing PRs related to Indy wrappers with pointers to Aries language libraries
 - LibVCX support for some Aries protocols
- Ursa 0.3.0 release in November
 - Updated BLS signature (multi-signatures, small-BLS)
 - Compilation optimization for specific hardware
 - Rest of predicates for Anoncreds 2.0 and delegatable credentials

Agenda

- Issue Game: Can we close this? (15 min - Sam Curren) - issues (as time permits): [#198](#), [#130](#), [#41](#), [#114](#)
- Use of `please_ack` in the `issue_credentials` protocol (15 min - Stephen Curran) - [presentation](#)
- Connectathon Update
 - Aries Interop Profile 1.0.0 - Stephen Curran - [presentation](#)
 - Community Coordinated Update - [RFC](#)
 - Testing
 - Biometrics
 - Shared Library Development
 - Schema 2.0
 - Inline Keys
 - DIF DIDComm WG
- 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
- 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](#)
- [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](#))

Action items

Call Recording

File	Modified
Multimedia File GMT20191211-200330_Aries-WG-C_2220x2008.mp4	Dec 12, 2019 by Sam Curren
Multimedia File GMT20191211-200330_Aries-WG-C.m4a	Dec 12, 2019 by Sam Curren
Text File GMT20191211-200330_Aries-WG-C.txt	Dec 12, 2019 by Sam Curren

[Download All](#)