

2019-12-18-B Aries Working Group Call (US afternoon)

Summary:

Planned Topics:

- Transition Message Types
- Connectathon Topics (continued)

Note: This call is being recorded.

Date

18 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 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>
- [Steve McCown](#) (Anonymo Labs) <smccown@anonymo.com>
- [Troy Ronda](#) (SecureKey) <troy.ronda@securekey.com>
- [Baha A Shaaban](#) (SecureKey) <baha.shaaban@securekey.com>
- [Stephen Curran](#) (Cloud Compass/BC Gov) <swcurran@cloudcompass.ca>
- [Ken Ebert](#) (Sovrin Foundation) <ken@sovrin.org>
- [John Callahan](#) (Veridium) <jcallahan@veridiumid.com>
- [Paul Knowles](#) (Dativa) <paul.knowles@dativa.com>
- [Filip Burlacu](#) (SecureKey) <filip.burlacu@securekey.com>


Welcome / Introductions

Announcements

- New Indy/Aries/Ursa edX course, now online - [enroll now!](#)
- Dec 25th and Jan 1st calls canceled for holidays
- 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 Protocol Test Suite
- Aries Shared:
 - Aries KMS
 - Verifiable Data Registry Interface (VDRI) library
 - Other Core Libraries (pack / unpack)
- Aries-CloudAgent-Python ([bc.gov](https://bcgov.github.io)) - Latest is [Release 0.4.0](#) on PyPi - some internal breaking changes regarding plugins
- Aries-Framework-Go (Troy) #aries-go
 - [2019-12-17 Framework Go Weekly Planning](#)
 - [RFC implementation status and Wishlist](#)
 - Continuing efforts on routing & relays, [crypto/kms](#), WebAssembly, generic JSON messages, [JWE envelopes](#), verifiable credential Go package.
 - 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](#).
- Aries-SDK-Ruby (Jack)
- Aries-Framework-DotNet (Tomislav)
- Aries-StaticAgent-Python - Now up to 0.6.1; [more details](#)
- Aries-Toolbox
- Aries-SDK-Python - Wrapper from JeromK and SBICA?
- 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
 - LibVCX 0.5.0 with Aries protocol support released today.
- 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
 - 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 - Sam Curren) - issues (as time permits):
 - [#256](#), [#144](#), [#239](#), [#146](#)
- [Transition Message Type to HTTPs](#) (15 min - Stephen Curran)
- Connectathon Update (Continued)
 - Biometrics
 - Shared Library Development
 - Schema 2.0
 - Inline Keys
 - DIF DIDComm WG
- HTTP over DIDComm
- Open Discussion / Next Week Topics

Next Week

Future Topics

- [RFC 351](#) (Generic JSON communication protocol). Use cases for [RFC 335](#) (HTTP over DIDComm).
- 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 Mitwicky](#)(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 Mitwicky](#)
- [Update message type and protocol identifier to https.](#) (and protocol documentation hosting.)
- Formal protocol verification techniques
 - https://github.com/SvenHamann90/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 GMT20191218-200400_Aries-WG-C.m4a	Dec 19, 2019 by Sam Curren
Text File GMT20191218-200400_Aries-WG-C.txt	Dec 19, 2019 by Sam Curren
Multimedia File GMT20191218-200400_Aries-WG-C_2020x2018.mp4	Dec 19, 2019 by Sam Curren

[Download All](#)