

2019-12-04-A Aries Working Group Call (US morning)

Summary:

- Connect-a-thon update
 - Discussions of the Aries Protocol Test Suite
 - Next steps with Aries Shared Libraries
 - Roadmap for Aries contributions over the next three months
- Trusted Digital Web

Note: This call is Recorded. Recordings posted at the bottom of the page.

Date

04 Dec 2019 (7AM Los Angeles, 10AM New York, 3PM London, 4PM CET, 18H Moscow)

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 (Employer) <email>
- Troy Ronda (SecureKey) <troy.ronda@securekey.com>
- [John Jordan](#) (Province of British Columbia) <john.jordan@gov.bc.ca>
- [Stephen Curran](#) (Cloud Compass Computing / Province of British Columbia) <swcurran@cloudcompass.ca>
- [Marvin Berstecher](#) (esatus AG) <m.berstecher@esatus.com>
- [Wolfgang Lamot](#) (difacturo) <wolfgang.lamot@difacturo.com>
- [John Callahan](#) (Veridium) <jcallahan@veridiumid.com>
- [Kalyan Kulkarni](#) (AyanWorks) <kalyan@ayanworks.com>
- [Bernardus Kurnia](#) (Binus University) <bernardus.kurnia@binus.ac.id>
- [Carl DiClementi](#) (Factom Inc) <carl@factom.com>
- [Richard Esplin](#) (Evernym) <richard.esplin@evernym.com>
- [Ken Ebert](#) (Sovrin Foundation) <ken@sovrin.org>
- [Adam Burdett](#) (Sovrin Foundation) <adam@sovrin.org>

Welcome / Introductions

Announcements

- Aries Workshop/Connectathon December 3-5 in Provo, Utah - Dates Confirmed, Food Sponsors welcome!
- Hyperledger edX course - [Introduction to Hyperledger Sovereign Identity Blockchain Solutions: Indy, Aries & Ursa](#)

Related Calls

- Previous Aries Working Group calls
- Identity Implementors Working Group call
 - Main place to get project updates, release status, and announcements.

Release Status and Work Updates

- Aries Protocol Test Suite
- Aries-KMS
- Verifiable Data Registry Interface (VDRI) library
- Other Core Libraries (pack / unpack)
- Aries-CloudAgent-Python (bc.gov) - Latest is [Release 0.3.5](#) on PyPi
- Aries-Framework-Go (Troy) #aries-go

- [2019-12-03 Framework Go Weekly Planning](#)
 - Investigating usage of [Tink](#) to support a native Go KMS (also supports other languages).
 - Continuing efforts on routing, duplex transport (transport return route), WebAssembly, [JWE envelopes](#).
- 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-SDK-JavaScript
- 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

RFC Progress

- Rich Schema RFC headed to an APPROVED status, Troy had some comments on how the Link Secrets tie to W3C spec.
- Proposal to renumber RFC 0289
- Progress on [JWE envelopes](#) (RFC 334).
- Draft RFC on [HTTP over DIDComm](#).

Other Business

- Connect-a-thon update
 - Aries Interop profile
 - LibVCX and Aries
 - KERI for key management: <https://arxiv.org/pdf/1907.02143.pdf>
 - DIDComm Semantics
- Progress on the Aries Protocol Test Suite, Sergey M.
 - Progress on the Protocol Test Suite: <https://github.com/hyperledger/aries-protocol-test-suite>
 - Alternative approach presented by Faber College (a.k.a. BC) <https://github.com/ianco/aries-agent-test-harness>
- Next steps with LibIndy evolution to an Aries model
 - Indy Resolver becomes Indy-Aries-VDRI
 - Indy Anoncreds becomes Aries-Creds-Anoncreds
 - Indy Pack / Unpack becomes Aries-Shared-Util
 - Indy Wallet becomes Aries-Shared-KMS
 - Aries-Shared-KMS-SQLite
 - Aries-Shared-KMS-PostgreSQL
 - Don't wait for resolver interfaces to standardize as RFCs
- Question about Aries-SDKs versus Aries-Frameworks
- Trusted Digital Web
 - Further discussion on the Semantics call December 10 see #indy-semantics at chat.hyperledger.org
 - <https://hyperonomy.com/2019/12/03/trusted-digital-web-first-trusted-web-page-delivered-today-dec-3-2019/>

Future Topics

- Next call
 - Aries KMS design
 - Define approved algorithms
 - Define plugin interface
 - 3rd party libraries we could leverage:
 - Google Tink as an encryption library
 - Hubs vs Agents
 - <https://www.hyperledger.org/blog/2019/07/23/rhythm-and-melody-how-hubs-and-agents-rock-together>
- Other:
 - Status and future of wallet query language
 - IOT best practices (Robert Mitwicki, Adam Burdett, Lohan Spies)
 - DID Resolution W3C and Sam's concerns: <https://github.com/hyperledger/aries-rfcs/issues/130>
 - Architecture of Aries Verifiable Credentials Proof Formats (Mike Lodder)

Action items



Call Recording

File	Modified
Text File GMT20191204-150509_Community-.txt Chat transcript	Dec 04, 2019 by Richard Esplin
Multimedia File GMT20191204-150509_Community-_1552x1080.mp4 Call recording	Dec 04, 2019 by Richard Esplin

[Download All](#)