

2020-03-25-B Aries Working Group Call (US afternoon)

Summary:

- Issue Game
- Mediator Repos
- DIDExchange Progress
- Issue Credential v2.0

Note: This call is being recorded.

Date

25 Mar 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>
- [George Aristy](#) (SecureKey) <george.aristy@gmail.com>
- [Sam Curren](#) (Independent) <telegramsam@gmail.com>
- [Stephen Curran](#) (Cloud Compass Computing Inc./BC Gov) <swcurran@cloudcompass.ca>
- [Richard Esplin](#) (Evernym) <richard.esplin@evernym.com>
- [Adam Burdett](#) (did.report) <burdettadam@did.report>
- [Nathan George](#) (Independent) nathan@ngeorge.org
- [Steve McCown](#) (Anonymome Labs) <smccown@anonymome.com>
- [Echo Harker](#) (Evernym) <echo.harker@evernym.com>
- [Brent Zundel](#) (Evernym) <brent.zundel@evernym.com>
- [Lynn Bendixsen](#) (Independent) <lynn.bendixsen@gmail.com>
- [Troy Ronda](#) (SecureKey) <troy.ronda@securekey.com>
- [John Callahan](#) (Veridium) <jcallahan@veridiumid.com>
- [Scott Zwierzynski](#) (Chainyard) <scott.zwierzynski@chainyard.com>

Welcome / Introductions

Announcements

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

Related Meetings Review

- Ursa -
 - Hashed curve stuff
- Semantics - yesterday's call (03/17) - [Notes](#)
 - (i.) Update: The Human Colossus Foundation: Synergy for a Decentralized Data Economy
 - (ii.) Discussion: Resource DID / DRI - What properties are required and can it be kept in the DID space?
 - Next meeting: 03/31 (Tuesday)
- [DID UX Call](#) - Slack/Mailing list - details in the shared document as well minutes and additional information, currently focus on Purpose Based Services
 - F2F Meeting meetup
- [SSI in IoT WG](#)
- Indy Contributors - [Richard Esplin](#) (Mon) - [Notes](#) (Focus on [supporting Indy Networks](#), including troubleshooting a Sovrin issue)
- Identity WG / Identity WG Implementer calls (Wed / Thurs)
- DIF DIDComm WG - Monday's at Noon US/Pacific

Upcoming Releases and Work Updates

- Aries Protocol Test Suite
 - No updates this week (contributions welcome)
- Aries Shared:
 - indy-vdr (Andrew Whitehead) <https://github.com/hyperledger/indy-vdr>
 - Remaining work: Design doc, FFI, testing, CI / CD
 - As an Aries interface becomes standardized, will add that API layer
 - Integrating into LibIndy in a separate branch, goal is to release in April/May
 - indy-credx / aries-credx
 - <https://github.com/sovrin-foundation/aries-credx-framework-rs>
 - <https://github.com/andrewwhitehead/indy-credx>
 - Ran a branch of ACAPy with Aries Credx instead of LibIndy
 - Aries-Shared-Util
 - Pack / Unpack
 - Not started yet
 - Aries-KMS
 - [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
- Aries-CloudAgent-Python (BC Gov)
 - 0.4.5 presentation verification fixes
 - Revocation based on anoncreds 1.0 has been merged into master and will be in the next release.
 - Because it uses tails files, use case support will be limited - just where the tails file is very small (e.g. 25k credentials)
 - Currently testing with mobile agents to give feedback on process, tweaking the API to provide controller control over the process.
- Aries-Framework-Go (Troy) #aries-go
 - Issue credential protocol with [BDD tests](#).
 - Started work on out-of-band and present proof protocols.
- Aries-SDK-Ruby (Jack)
 - Added genesis block parameterization via Rails encrypted creds
 - Updating <https://github.com/johncallahan/ruby-jsonld-signatures> (for verifiable credential use)
 - Working on developer use case via IEEE 2418.6 Identity subgroup on Vaccination records <https://github.com/p2418-6-identity/community>
- Aries-Framework-DotNet (Tomislav)
- Aries-StaticAgent-Python
- Aries-Toolbox
 - Payments admin protocols
 - Intended for use with various payment methods
 - Initial support for Sovrin test tokens in ACA-Py Plugin
 - Updates to Connection and Invitation admin protocols complete
- 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
 - 0.4.0 scheduled for late March
 - Hash to curve
 - Updates to AMCL wrapper

Agenda

- Mediator Repo Strategy - Sam
 - Mediators are a specific type of cloud agent
 - [Example mediator in LibVCX code contributed by ABSA](#) (could be extracted and stand alone)
 - Documentation (Readme files) should note that a mediator is not always functionally required.
 - verbose option: Mediators and Relays RFC
 - terse option: a paragraph or two. Copied to each repo, or as an anchored link in the above RFC?
 - aries-mediator-[language]? languages ready: go, dotnet, rust (absa)
 - binary & docker image that wraps an existing framework? (e.g., aries-mediator-go as an instance of aries-framework-go)
- DIDExchange Repo Progress
 - OOB Linked In ([PR 454](#))
 - Signed Attachments ([PR 456](#))
 - Reuse-accepted ([PR 455](#))
 - What's missing?
 - Role Names ([Issue 457](#))
- Issue Credential V2.0 ([Slides](#)) - Stephen
- Issue Game: Can we close this? (15 min)
- Open Discussion / Next Week Topics

Next Week

- Out-of-Band Rollout
 - Use with Connections
 - Community Coordinated Update, switching from Connections Invitations to OOB Invitations?
- Issue Credential Continued....?

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 (using [Tamarin](#))
 - 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 GMT20200325-190325_Aries-WG-C_2512x2004.mp4	Mar 26, 2020 by Sam Curren
Multimedia File GMT20200325-190325_Aries-WG-C.m4a	Mar 26, 2020 by Sam Curren
Text File GMT20200325-190325_Aries-WG-C.txt	Mar 26, 2020 by Sam Curren

[Download All](#)