

# 2020-02-26-A Aries Working Group Call (AMER morning)

## Summary:

- Work updates
- Progress on Rich Schemas
- Plans for CI / CD
- Plans for credx libraries

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

## Date

26 Feb 2020 (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 Updegrave of the firm of Gesmer Updegrave LLP, which provides legal counsel to the Linux Foundation.

## Attendees

- Name (Employer) <email>
- Troy Ronda (SecureKey) <troy.ronda@securekey.com>
- [Richard Esplin](#) (Evernym) <richard.esplin@evernym.com>
- [Ken Ebert](#) (Sovrin) <ken@sovrin.org>
- [Stephen Curran](#) (Cloud Compass/BC Gov) <swcurran@cloudcompass.ca>
- [Echo Harker](#) (Evernym) <echo.harker@evernym.com>
- [George Aristy](#) (SecureKey) <george.aristy@securekey.com>
- [Steve McCown](#) (Anonymome Labs) <smccown@anonymome.com>
- [Sam Curren](#) (Sovrin Foundation) <sam@sovrin.org>

## Welcome / Introductions

## Announcements

- Hyperledger Global Forum: In person meetings
- Hyperledger Diversity, Civility, and Inclusivity [Survey](#)
- [IIW](#) April 28-30

## Related Calls

- Previous Aries Working Group calls
- DIF DIDComm WG Call: [Rolling Agenda](#).
- Identity Implementors Working Group call
  - Main place to get project updates, release status, and announcements.

## Release Status and Work Updates

- Aries Protocol Test Suite
  - Issue, credential, and proof tests are merged.
- Aries Shared:
  - indy-vdr (Andrew Whitehead) <https://github.com/andrewwhitehead/indy-ledger-client>
    - Basically usable
    - Remaining work: Design doc, FFI, and testing
    - Will migrate repo to Hyperledger
    - As an Aries interface becomes standardized, will add that API layer
  - indy-aries-anoncreds / indy-creds indy-credx and aries-credx

- <https://github.com/sovrin-foundation/aries-credx-framework-rs>
  - Aries-Shared-Util
    - Pack / Unpack
    - Not started yet
  - Aries-KMS
    - Mike Lodder working on documentation and architecture as an Aries RFC (KMS architecture) and Ursa RFC (API)
      - Differs from Indy Wallet architecture by separating out auth and access control. Intention is to ensure a smooth transition from Indy.
      - Ability to export keys under certain conditions (metadata is set upon key creation)
    - Mike and Cam's aries-core-rs aries-kms-mayaguez
      - <https://github.com/sovrin-foundation/aries-kms-rs>
        - Evolution from lox
        - Will include a default storage that is not a different implementation from the plugins
    - Indy wallet crate might move to start another aries-kms implementation aries-kms-vostok
- Aries-CloudAgent-Python (bc.gov)
  - Likely releasing 0.4.3 shortly - an update is needed for TAA handling
- Aries-Framework-Go (Troy) #aries-go
  - Enable common JavaScript API for both WASM and REST controller APIs.
  - Verifiable Credential controller APIs (validation and storage).
  - [Preparing 0.1.2 release](#)
- Aries-SDK-Ruby (Jack)
  - Added DID/Verkey sign\_and\_submit to [aries\\_sdk\\_ruby](#) and published new [gem](#) (0.0.8)
  - Created [aries-rails-docker](#) experiment that support Rails 4 with Indy 1.8.1 on Heroku & Dokku
- Aries-Framework-DotNet (Tomislav)
  - Release last week for Aries compatibility with ACApy and LibVCX (RFC 0094)
- Aries-StaticAgent-Python
- Aries-Toolbox
  - Added basic message admin
  - Working on a getting started video
- Aries-SDK-Java
- Aries-Framework-JavaScript / Aries-SDK-JavaScript
  - Started regular meetings: [Framework JS Meetings](#)
- Rich Schemas and W3C Verifiable Credentials (Brent & Ken)
- Ursa
  - 0.3.2 released in February, includes key exchange methods (can replace libsodium)

## RFC Progress

## Other Business

- Progress on Rich Schemas / W3C Verifiable Credentials [Ken Ebert](#)
  - [Collaboration session](#)
  - Rich Schemas Roadmap:
    - HIPE / RFCs (50% done)
      - Issuance in DIDComm
      - Proof in DIDComm
      - Mapping (Alex)
      - Cred Def (Alex)
      - Presentation Def (Ken and Brent)
      - Presentation (Ken and Brent)
      - Verifiable Credential (Alex)
      - Update existing HIPEs/RFCs (Alex)
      - HIPEs/RFCs for new objects:
    - Indy Node implementation (95% done) (Alex)
    - Indy-vdr (Andrew N)
      - Prerequisite: CI / CD for indy-vdr, and integration into Indy SDK
    - aries-credx (Andrew N and Echo)
      - create\_w3c\_cred
      - sign\_w3c\_cred
      - verify\_w3c\_cred
      - create\_presentation
  - Milestones
    1. Issue a credential
    2. Verify using a presentation definition with ZKP signature
  - Aries-Framework-Go already supports W3C VC's: JSON-LD and JWTs
  - Avoid the term "Rich Schema" in artifacts and code.
- Merge indy-credx with aries-credx?
  - <https://github.com/sovrin-foundation/aries-credx-framework-rs>
    - Generic APIs that are pluggable
    - Test vectors for interop
      - W3C test suite doesn't have encodings / mappings in the data model
      - But should test against the W3C test suite for the shape of the data model
      - aries-framework-go W3C test suite CI: <https://github.com/hyperledger/aries-framework-go/actions?query=workflow%3Atest-suite>
  - <https://github.com/andrewwhitehead/indy-credx>
    - Anoncreds 1.0 won't have the W3C credential container
- Indy VDR is moved to Hyperledger

- <https://github.com/hyperledger/indy-vdr>
- CI / CD Aries shared libraries
  - Prefer GitHub Actions.
    - Use GitHub Actions Runner for iOS and Android hosted by the Sovrin Foundation.
    - Can easily migrate to Azure Pipelines or Circle CI if needed.
  - Aries-Framework-Go is using both GitHub Actions and (to a limited extent) Azure Pipelines
    - Azure Pipelines supported deployments that GitHub Actions didn't (likely does now)
    - Azure Pipelines worked better for heavy tests: more computationally intensive and parallel
  - We plan to reduce the number of architectures. Won't support old devices.
- When building Aries Util (pack / unpack) will migrate from LibSodium to Ursa key exchange?
  - Probably, but need additional testing.
- BC.gov is using Pyo3 as well as FFI in shared libraries
  - Python extension written in Rust that wraps crate directly. Improves performance and security. Allows multiple threads.
  - Take a different approach for FFI? Raw pointers or buffer paradigm instead of serialized strings
  - <https://github.com/andrewwhitehead/indy-credx/blob/master/wrappers/python/src/buffer.rs>

## Future Topics

- Next Meeting (March 11)
  - Aries KMS design [Mike Lodder](#)
    - Architecture RFC
    - 3rd party libraries we could leverage:
      - Google Tink as an encryption library used in the KMS for aries-framework-go
- Other:
  - Formal verification ([Sven Hammann](#))
  - Where should we document interoperability results (AIP 1.0)? A page in this wiki space?
  - Hubs vs Agents
    - <https://www.hyperledger.org/blog/2019/07/23/rhythm-and-melody-how-hubs-and-agents-rock-together>
  - 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
Multimedia File zoom_0.mp4	Feb 26, 2020 by Richard Esplin
Text File meeting_saved_chat.txt	Feb 26, 2020 by Richard Esplin
Multimedia File audio_only.m4a	Feb 26, 2020 by Richard Esplin

[Download All](#)