

# 2020-07-01-A Aries Working Group Call (AMER morning)

## Summary:

- Work updates
- Transferable reputation via VC (Mike Richardson - EuroLedger)
  - Topic to discuss:
    - Proxy Issuer Wallet: is this a bit too much of a centralised data store?
    - Website Authentication, use of Trinsic connection Ids, or DIDs for user passcode?
    - Lack of revocation notifications: is this a problem?
    - Synchronizing upstream and downstream platforms (ie issuer and verifier) where credentials change
    - Wallet management: are we in danger of "credential proliferation"?
- Optional: Wallets - do we need certification and who can do it? [Robert Mitwicki](#)
- Other businesses

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

## Date

17 Jun 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 Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.


## Attendees

- Name (Organization) <email>
- Robert Mitwicki [Robert Mitwicki](#) (The Human Colossus Foundation) - [robert.mitwicki@humancolossus.org](mailto:robert.mitwicki@humancolossus.org)
- Mike Richardson (EuroLedger) <emerysolutions@yahoo.co.uk>
- Victor Martínez (SICPA) <victor.martinez@sicpa.com>
- Steve McCown (Anonymome Labs) <smccown@anonymome.com>

## Welcome / Introductions

## Announcements

- Trust Over IP - Decentralized Semantic Working Group - Was Approved - First call 26/06 :
- eSSIF-Lab: [https://essif-lab.eu/?page\\_id=134](https://essif-lab.eu/?page_id=134)

 Unknown macro: 'lref-gdrive-file'

## Related Calls

- Previous Aries Working Group calls
- DIF DIDComm WG Call: [Rolling Agenda](#).
- Identity Implementors Working Group call
  - [2020-07-02 Identity WG Implementers Call](#)

## Release Status and Work Updates

- Aries Protocol Test Suite
  - One agent under test
  - Issue, credential, and proof tests are merged.
- Aries Agent Test Harness
  - Test compatibility between any two agents

- [https://github.com/bcgov/aries-agent-test-harness\\_](https://github.com/bcgov/aries-agent-test-harness_)
- Aries Shared:
  - Aries Shared:
    - indy-vdr (Andrew Whitehead) <https://github.com/hyperledger/indy-vdr>
      - Nearing release 0.6(?) - most work complete that was needed: Design doc, FFI, testing, CI / CD
        - CI - GitHub actions runs unit tests and basic integration tests
        - CD not there
        - No design doc, but crate docs
        - Rich Schema merged and behind a feature flag
        - Refactoring PR not merged - cleanup, internal simplification, crate docs
    - indy-credx - <https://github.com/bcgov/indy-credx>
      - Experimental ACA-Py branch created that can do credential exchange with indy-credx
    - indy-shared-rs - <https://github.com/bcgov/indy-shared-rs>
      - Shared features across indy-vdr and indy-credx
      - pack/unpack on Ursa (not libsodium)
    - aries-credx
      - <https://github.com/sovrin-foundation/aries-credx-framework-rs>
        - 6 most common attribute encodings (but not anoncreds 1 attribute encoding)
      - Can make a non-revocable credential and create proofs.
    - Aries Secure Storage initiatives:
      - Mike working on documentation and architecture as an Aries RFC (KMS architecture) and Ursa RFC (API)
        - PR is submitted: <https://github.com/hyperledger/aries-rfcs/pull/440>
      - Mike and Cam's work aries-kms-mayaguez - Postgres backend for credential storage
        - <https://github.com/sovrin-foundation/aries-kms-rs>
          - Persistence work allows plugging in any database engine.
          - Focus is using an external enclave.
      - aries-kms-vostok - indy-wallet capabilities moved to an Aries base
        - Andrew also working on that
- Aries-CloudAgent-Python (bc.gov)
  - Release 0.5.1 is on PyPi.
  - Revocation support added and tested with Streetcred and esatus Mobile Agents; major/minor version handling
- Aries-Framework-Go (Troy) #aries-go
  - Implementing the [Out-Of-Band protocol](#)
  - Implementing issue-credential and present-proof protocols
  - Edge agent in work based aries-framework-go using WASM with support for DIDs, VCs and DIDComm support being added
- 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
  - PR for Connections Update
  - Converted to a web application by [Robert Mitwicki](#) - repo <https://github.com/thclab/aries>
  - Upcoming cleanup items
- Aries-SDK-Java
- Aries-Framework-JavaScript
  - Started regular meetings: [Framework JS Meetings](#)
  - Current focus is on mediator use case (NodeJS)
- Rich Schemas and W3C Verifiable Credentials (Brent & Ken)
  - Some work has been done to support the W3C Verifiable Credentials Data Model specification
- Aries-MobileAgent-Xamarin (Aries MAX)
  - Evolution of the open source mobile agent (Matr Global's OSMA)
  - <https://github.com/hyperledger/aries-mobileagent-xamarin>
- Ursa
  - 0.4.0 scheduled for late March
    - Improved hash to curve algorithm
    - Updates to AMCL wrapper
  - To replace libsodium, need to have a replacement for the anoncrypt / authcrypt sealed box for pack / unpack.
    - Can be done in Ursa with two steps, but might add as a single function call.

## Agenda:

## RFC Progress

## Other Business

## Future Topics

- Next Meeting
- Other:
  - 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
  - DID Resolution W3C and Sam's concerns: <https://github.com/hyperledger/aries-rfcs/issues/130>
  - Architecture of Aries Verifiable Credentials Proof Formats (Mike Lodder)

- Connectionless
- KERI - deep dive / transaction family / Notary groups /
- Chain credentials 0104-chained-credentials

## Action items



## Call Recording

File	Modified
------	----------

