CARDEA

Interop-a-thon

March 17, 2022
8:00 am MDT - 12:00 pm MDT

LF PUBLIC HEALTH

Overview

CARDEA

Cardea is now being piloted to share COVID-19 test results, and vaccine and trusted traveler credentials.

To drive interoperability among these projects, Cardea hosted the second four-hour virtual Interoperability “hack-a-thon style event” on March 17, 2022. (the first was held September 9, 2021)

The maintainers of Cardea stood up a test environment including an Issuer, Mobile, Mediator, Government, and Verifier Agents for participants to test against, as well as new features such as out of band invitations and machine readable governance.

Goals

CARDEA

Drive interoperability! Interoperability is the key to decentralized identity's growth into a network of networks. This event tested Hyperledger Indy based projects; future interop-athons will cover other signature styles.

Participants had the opportunity to:

- Test different vendor solutions interoperating with the Cardea reference implementation
- Test vendor solutions interoperating directly with each other
- Test out of band invitations
- Test machine readable governance
- Discover areas of friction
- Create a roadmap of changes to improve interoperability
- Publish test results

LF PUBLIC HEALTH

By the numbers

CARDEA

- Received 14 project submissions *(+2 from previous event)*
- ~13 interop-athon participants *(- 14 from previous event)*
- Projects brought a variety of solutions to issue, verify, and hold verifiable credentials, using a reference implementation provided by Cardea
- The default network was Indicio TestNet.
- Each project had the opportunity to test against the Cardea reference implementation and against as many other participants as possible.
- In total, 18 tests were conducted. *(-12 from previous event)*

Registered Participants

CARDEA

- HealthBlocks*
- IdRamp
- Procivis AG
- Silibrain*
- lissi @ Main Incubator GmbH
- ATB Ventures*
- OpenHealth*
- Ayanworks Technology Solution Pvt. Ltd*
- SITA
- Liquid Avatar
- Government of BC*
- Petri Dish Development Inc.*
- IDLab

LF PUBLIC HEALTH

* = did not participate

Testing

CARDEA

- Indicio set up a reference implementation including:
  - Cardea Issuers
  - Cardea Mediator
  - Cardea Mobile wallet
  - Cardea Verifier
  - Out Of Band Invitations
  - Machine Readable Governance
- Using Zoom breakout rooms, each participant had the opportunity to begin the day testing against the Cardea reference implementation.
- Participants also had the chance to meet in pairs to test against one another, with an Indicio trained staff member to facilitate.

Workflow

Out-of-Band Invitations

- One of the enterprise agents can be used to display a QR code based on an out-of-band invitation URL. This is done by clicking on the “Display OOB” button on the home page. You can copy the invitation URL from the Console Log tab of your browser’s dev tools if you need it instead of the QR code.
- The invited agent scans the QR code or copies and pastes the invitation URL into a form field and accepts the invitation. (NOTE: For Cardea, only the enterprise agents support OOB at the moment)
- Either the connection process proceeds and a connection is formed (using the connections v. 1.0 protocol as the handshake protocol; you should see an active connection in the list of contacts) or error messages should appear in the enterprise agent logs.

Workflow

Health Credential Issuance

- Lab Enterprise Agent displays an invitation
- Holder Agent connects using the invitation
- Lab Enterprise Agent requests identity information using the present-proof v. 1 protocol
- Holder Agent responds with a self-attested identity proof
- (Optional) Lab Enterprise Agent issues a lab_order credential
- (Optional) Lab Enterprise Agent checks to make sure a connection (contact) has been issued a lab_order
- Lab Enterprise Agent issues a lab_result, vaccine, or vaccine_exemption credential to the Holder Agent

Workflow

CARDEA

Trusted Traveler Issuance

- Government Enterprise Agent displays an invitation
- Holder Agent connects using the invitation
- Government Enterprise Agent requests identity information using the present-proof v. 1 protocol
- Holder Agent responds with a self-attested identity proof
- Government Enterprise Agent requests presentation of a lab_result, vaccine, or vaccine_exemption credential
- Holder Agent responds with the credential of its choice
- Government Enterprise Agent verifies the credential cryptographically and validates the following attributes (if you are trying to demonstrate a particular use case, you can validate more): a. lab_result must be “Negative” and lab_specimen_collected_date must be a Unix timestamp less than 3 days ago OR lab_result must be “Positive” and lab_specimen_collected_date must be a Unix timestamp more than 28 days ago b. vaccine: vaccine_series_complete must be “true” and vaccine_administration_date must be a Unix timestamp more than 14 days ago c. vaccine_exemption: exemption_expiration_date must be a Unix timestamp in the future.
- Government Enterprise Agent issues a trusted_traveler credential to the Holder Agent

Workflow

CARDEA

Trusted Traveler Verification

- Verifier Agent displays an invitation
- Holder Agent connects using the invitation
- Verifier Agent requests presentation of a trusted_traveler credential
- Holder Agent responds with its trusted_traveler
- Verifier Agent displays “Approved” or “Not Approved” depending on the result of the cryptographic verification (we recommend verifying trusted_traveler_expiration_date_time (Unix timestamp) is not in the past using a predicate proof).
- **For machine readable governance,** if the trusted_traveler was not issued by a trusted government issuer, the Enterprise Verifier Agent sends a basic message to the Holder Agent that states that the credential was not issued by a trusted issuer.

Success

CARDEA

- **Out of band** will be adopted by the Hyperledger Aries community (target: March 31). This interop-a-thon provided an opportunity for a first step in out of band implementation.
- **Machine readable governance** worked well to test validation of participants (issuers and verifiers). This is the first time MRG has been used in a practical setting. Machine readable governance is still extremely new and having the code to test against was a major milestone.
- Teams that prepared tools against existing standards using Cardea based agents were highly successful interoperating with other Cardea based agents
- Teams that used the Aries **protocols** and the agreed-upon schemas were able to participate in the ecosystem
- Teams that participated were able to benefit from cross- community troubleshooting and problem solving, expedited resolutions

Lessons Learned

CARDEA

- **Out of band**: We wrote but didn't adequately distribute or follow an interop profile. Connection ACK is required to complete connections in Cardea.The Hyperledger Aries RFC lists it as 'optional' and teams that interpreted it as such had difficulties completing this test.
    - Connection states in ACA-Py / Assumes another message is optional when in Cardea it is mandatory
- Some participants had mistakes in their implementation of the Hyperledger Aries protocols (e.g., invitation messages not base64URL encoded)
- The Q&A protocol was supposed to have workarounds available, but proved to be a blocker for some participants. Be careful including things that aren't being tested in the reference implementation
- We may want to have tests available for discrete operations instead of full workflows

Lessons Learned (cont'd)

CARDEA

- Although the reference implementation was provided earlier than previous events, it should be released as soon as possible.
  - Communicate what new features will be tested but also be specific about individual tasks that will be tested.
- The participation survey needs to be updated so the questions are harder to answer in ways that have multiple meanings (e.g., "what are you interested in testing?" could mean what do you have or what you want to test against)
  - Participants should be required to make organizers aware of the specific tools, networks, and features they will be prepared to test.
- Those who signed up and didn't come should be contacted to see what their obstacle or reason was for registering but not attending.
  - All participants should receive a post-event survey
- Office hours were not utilized by any participant.
  - Provide further opportunities for demo/education/workshops/direction ahead of time
  - Post-event outreach to be conducted by technical member of the community
  - Clearer communication about how the event is run and its benefits
- We should have note takers so the tech support staff can focus on running the room

Recordings and Notes Repo

CARDEA

Full event details and recordings are available

Recordings can be found here

Complete repository of testing notes can be found at the following links:

- Room 1
- Room 2
- Room 3
- Room 4
- Room 5
- Room 6

LF PUBLIC HEALTH

Code

CARDEA

- Cardea github https://github.com/thecardeaproject
- Agent URLs:
  - **Mobile Holder:** https://github.com/thecardeaproject/cardea-mobile-holder/releases/tag/1.1.0
  - **Health Issuer**: https://lab.cardea.indiciotech.io/
  - **Travel Issuer**: https://government.cardea.indiciotech.io/
    - Note: For the purposes of this test, a holder must send a message so the connection status is considered active. If the holder doesn't send demographics, the user must also edit the demographics before sending.
  - **Enterprise Verifier:** https://restaurant.cardea.indiciotech.io/
  - **Mobile Verifier:** https://github.com/thecardeaproject/cardea-mobile-verifier/releases/tag/1.0.2
- Cardea Schemas: https://github.com/thecardeaproject/cardea/tree/main/schemas

(*Interop profile: which protocols we'll be using + rfc references)

LF PUBLIC HEALTH