TRUST Over IP FOUNDATION

Decentralized Semantics WG Weekly Meeting

4 August 2020

THE LINUX FOUNDATION

Antitrust Policy Notice

- 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.

Agenda

1. Welcome (Paul—5 mins)
2. Newcomer Introductions (5 mins)
3. Task Force Updates (10 mins)
4. Rich Schema Object integration using OCA (Group discussion - 30 mins)
5. Indy Interop-athon (Paul/Robert—10 mins)
6. Logistics (Paul—5 mins)
    a. Chairs
    b. Meeting schedule

Newcomer Introductions

(30 seconds!)

1. Name
2. Location / time zone
3. Affiliation(s)
4. One-sentence summary of your interest in Decentralized Semantics (or one particular semantics-related issue you personally want to see solved)

Task Force Updates
(10 mins)

- Imaging TF (Scott/Moira)
- Medical Information TF (Scott/Moira)
- Notice & Consent TF (Mark/Sal)

Rich Schema Object integration using OCA
(30 mins)

Group discussion – Presenter: P. Knowles

https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0250-rich-schemas

Rich Schema *(Hyperledger Indy work):*

Definition -

The rich schemas and associated constructs are linked data objects that have an explicitly shared context. This allows for all entities in the ecosystem to operate with a shared vocabulary.

Because rich schemas are composable, the potential data types that may be used for field values are themselves specified in credential schemas that are linked to in the property definitions. The shared semantic meaning gives greater assurance that the meaning of the claims in a presentation is in harmony with the semantics the issuer intended to attest when they signed the credential.

Rich Schema *(Hyperledger Indy work):*

What do they offer? -

(i.) **Improved Predicate Proofs**

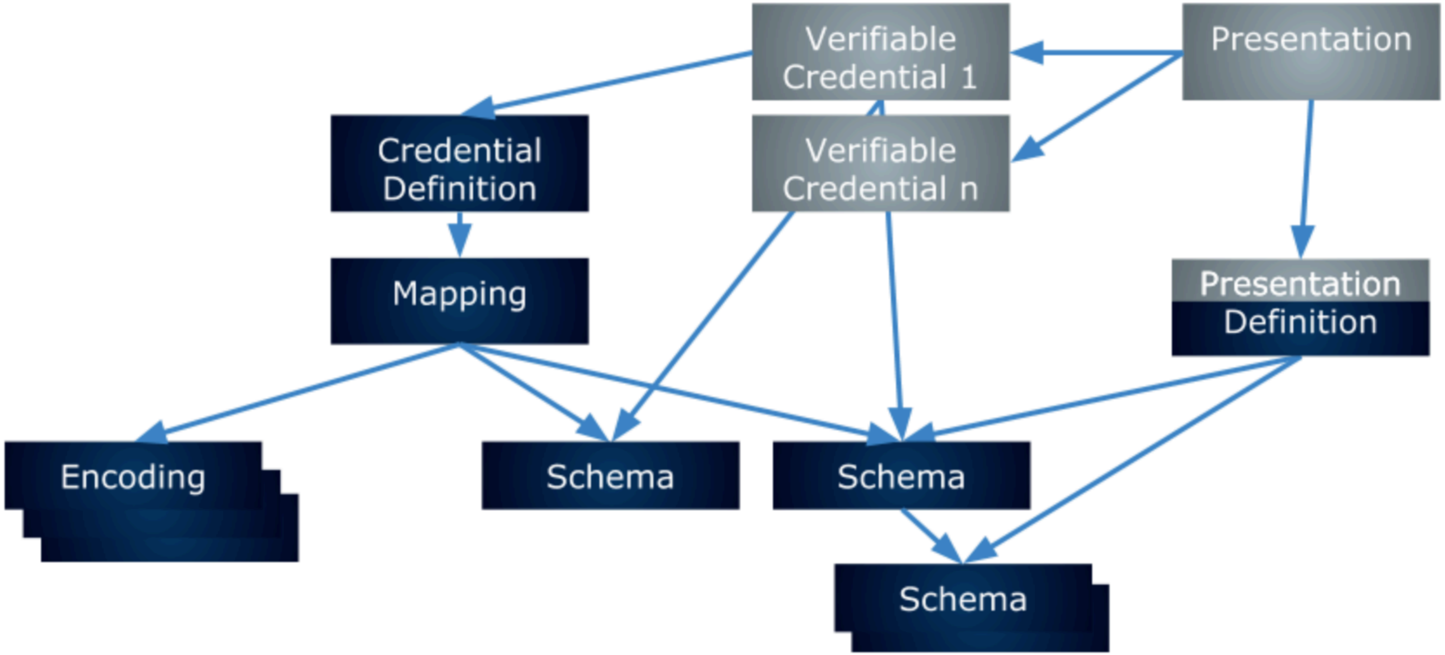
- Introducing standard binary-to-text encoding methods (e.g. Hyperledger Ursa) for most data types will enable predicate proof support. The Rich Schema work also introduces a mapping object that ties intended encoding methods to each credential schema attribute that may be signed so that an issuer will have the ability to canonically specify how the data they wish to sign maps to the signature they provide.

(ii.) **Use of JSON-LD**

- Each rich schema object will specify the extent to which it supports JSON-LD functionality, and the extent to which JSON-LD processing may be required.

Rich Schema *(Hyperledger Indy work):*

Object linkage -



Rich Schema *(Hyperledger Indy work):*

What new overlay types do we need? -

Rich Schema design includes a mapping object that ties intended binary-to-text encoding methods to each credential schema attribute that may be signed so that an issuer will have the ability to canonically specify how the data they wish to sign maps to the signature they provide.

(i.) **Order overlay**

- To be used for locking in a specific ordering sequence to credential schema attributes

(ii.) **Binary-to-text overlay**

- To be used to apply specific binary-to-text encoding definitions to credential schema attributes from pre-existing libraries (e.g. Hyperledger Ursa)

Rich Schema *(Hyperledger Indy work):*

What would this allow? -

... Zero-knowledge proof functionality

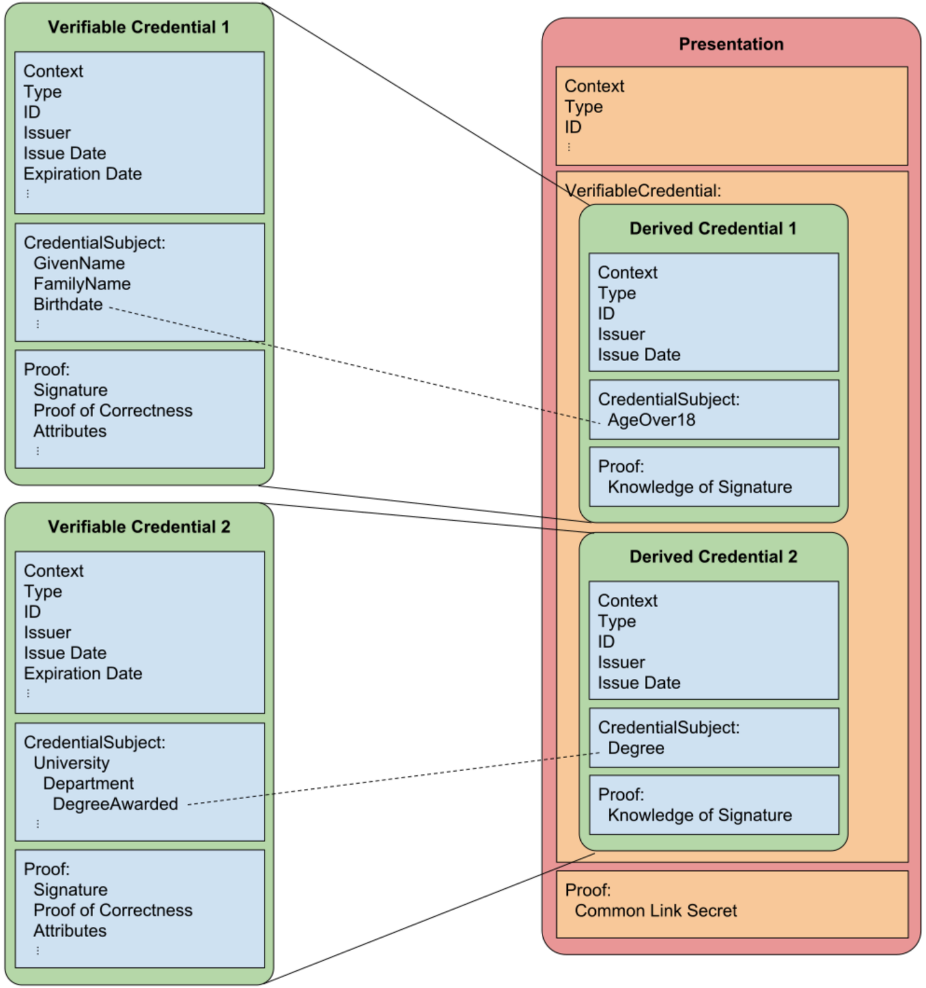
*In cryptography, a **zero-knowledge proof** or **zero-knowledge protocol** is a method by which one party (the prover) can prove to another party (the verifier) that they know a value x, without conveying any information apart from the fact that they know the value x.*

The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

Rich Schema

(Hyperledger Indy work):

Presentations -



Rich Schema *(Hyperledger Indy work):*

Links -

Aries RFC 0250: Rich Schema Objects -
https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0250-rich-schemas

Verifiable Credentials Data Model 1.0 -
https://w3c.github.io/vc-data-model/

Anoncreds Protocol -
https://github.com/hyperledger/indy-hipe/pull/109

Indy Interop-athon

(Proposed dates: September 1st & 2nd)

Robert Mitwicki, Human Colossus Foundation (15 mins)

Indy Interop-athon - Description

Leading SSI networks will be organizing an Indy Interoperability Conference (code name “Indy Interop-athon”) which will focus on the work needed to be done to the Hyperledger Indy and Aries code bases to make the network of networks a reality.

In addition to the benefits of further decentralization, resilience and value creation through cooperative network effects, interoperability also brings the goal of *Identity for All* one step closer, a mission which cannot be achieved with one network alone.

Details about the conference and registration …
https://wiki.hyperledger.org/pages/viewpage.action?pageId=36734079

Chairs

- As a Working Group, we elect our own chairs
  - At least one, and up to three
  - Two or three is recommended to spread out the load
- We can periodically rotate chairs as needed
- Volunteers now?

Meeting schedule

- Call timing
  - **ToIP Decentralized Semantics WG**

    Every Tuesday starting

    09:00 PT, 12:00 ET, 17:00 UK, 18:00 CET
- Next meeting
  - August 11th, 2020

TRUST Over IP FOUNDATION

Closing Q & A

THE LINUX FOUNDATION

Legal Notices

The Linux Foundation, The Linux Foundation logos, and other marks that may be used herein are owned by The Linux Foundation or its affiliated entities, and are subject to The Linux Foundation's Trademark Usage Policy at https://www.linuxfoundation.org/trademark-usage, as may be modified from time to time.

Linux is a registered trademark of Linus Torvalds. Please see the Linux Mark Institute's trademark usage page at https://lmi.linuxfoundation.org for details regarding use of this trademark.

Some marks that may be used herein are owned by projects operating as separately incorporated entities managed by The Linux Foundation, and have their own trademarks, policies and usage guidelines.

TWITTER, TWEET, RETWEET and the Twitter logo are trademarks of Twitter, Inc. or its affiliates.

Facebook and the "f" logo are trademarks of Facebook or its affiliates.

LinkedIn, the LinkedIn logo, the IN logo and InMail are registered trademarks or trademarks of LinkedIn Corporation and its affiliates in the United States and/or other countries.

YouTube and the YouTube icon are trademarks of YouTube or its affiliates.

All other trademarks are the property of their respective owners. Use of such marks herein does not represent affiliation with or authorization, sponsorship or approval by such owners unless otherwise expressly specified.

The Linux Foundation is subject to other policies, including without limitation its Privacy Policy at https://www.linuxfoundation.org/privacy and its Antitrust Policy at https://www.linuxfoundation.org/antitrust-policy. each as may be modified from time to time. More information about The Linux Foundation's policies is available at https://www.linuxfoundation.org.

Please email legal@linuxfoundation.org with any questions about The Linux Foundation's policies or the notices set forth on this slide.