



**TRUST**  
Over **IP**  
FOUNDATION

# Semantics WG Weekly Meeting

17 November 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 Updegrave of the firm of Gesmer Updegrave LLP, which provides legal counsel to the Linux Foundation.

## Membership Advisory

- › For the protection of all Members, active participation in working groups, meetings and events is limited to members, including their employees, of the Trust over IP Foundation who have signed the membership documents (including Trust over IP membership agreement as well as relevant working group charters) and thus agreed to the intellectual property rules governing participation.
- › If you or your employer are not a member, we ask that you not participate in meetings by verbal contribution or otherwise take any action beyond observing.

# Agenda

- › 1. Welcome (Paul—2.5 mins)
- › 2. Newcomer Introductions (Paul—2.5 mins)
- › 3. Task Force/Focus Group Updates (WG—5 mins)
- › 4. Suggested name and structure of the WG (Open—20 mins)
- › 5. Linking identifiers: Requirements and characteristics (Paul—10 mins)
- › 6. GitHub Projects (Steven—15 mins)
- › 7. Logistics and miscellaneous (Paul—5 mins)
  - › a. News from the Operations Team
  - › b. Leadership positions
  - › c. Meeting schedule

# Newcomer Introductions

## (30 seconds!)

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

# Task Force/Focus Group Updates

(5 mins)

- Imaging TF (Scott)
- Medical Information TF (Scott)
- ✓ OCA-FHIR FG (John/Mukund)
- Notice & Consent TF (Mark)

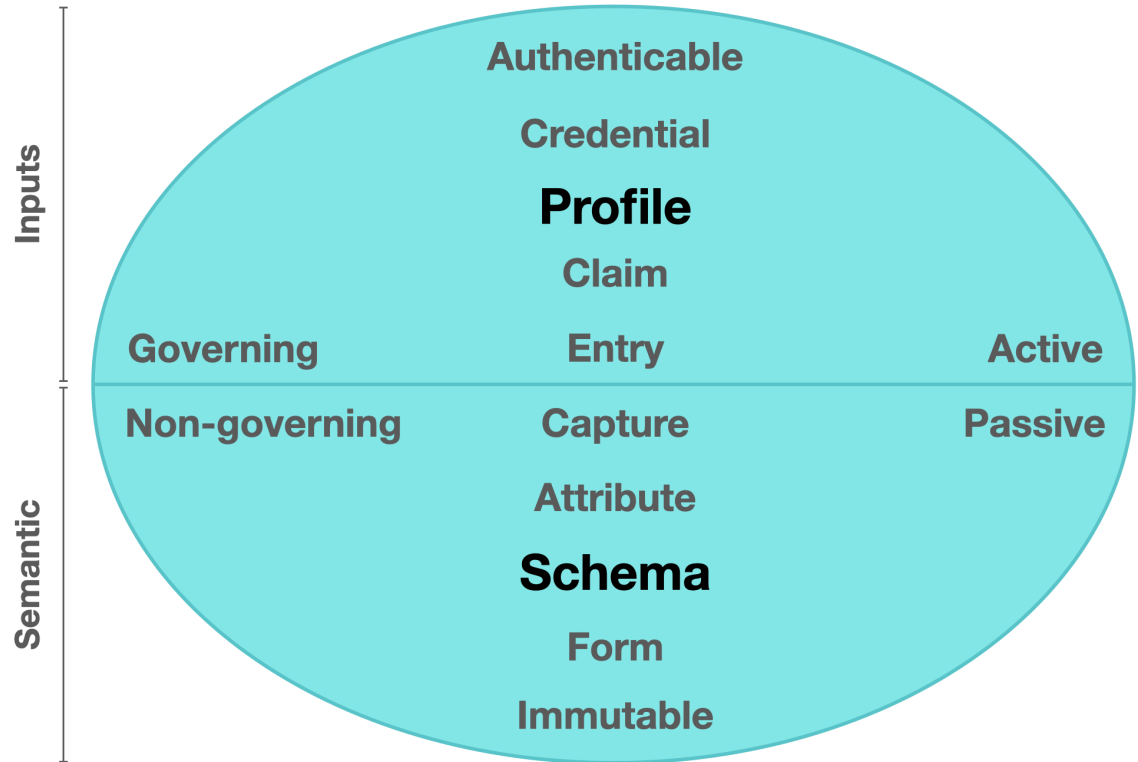
# Suggested name and structure of the WG (20 mins)

Open discussion

<https://docs.google.com/document/d/1EOSfkcAtMYyT4rlzpq-VWV1mQ90So9U9/edit#>

# Inputs and Semantics Working Group

A practical approach to further enable the adoption of the Trust over IP dual-stack architecture is to bring a balanced view of decentralized network paradigms to the overall mission of Internet-scale digital trust. All data inputs operated on by any process or system should be authenticable with the semantics providing meaning and context at the time of capture.



Ref.:

<https://humancolossus.foundation/blog/cjzegoi58xgpfzwxyrqlroy48dihwz>



## ISWG : Mission and scope

The mission of the WG is to define standards for Internet-scale deployment of: (i.) decentralized cryptographic key management; and (ii.) decentralized semantics.

The scope of the WG is to define specifications and best practices that bring cohesion to data entry (aka *Inputs*) and data capture (aka *Semantic*) processes and standards throughout the ToIP stack whether these standards are hosted at the Linux Foundation or external to it.

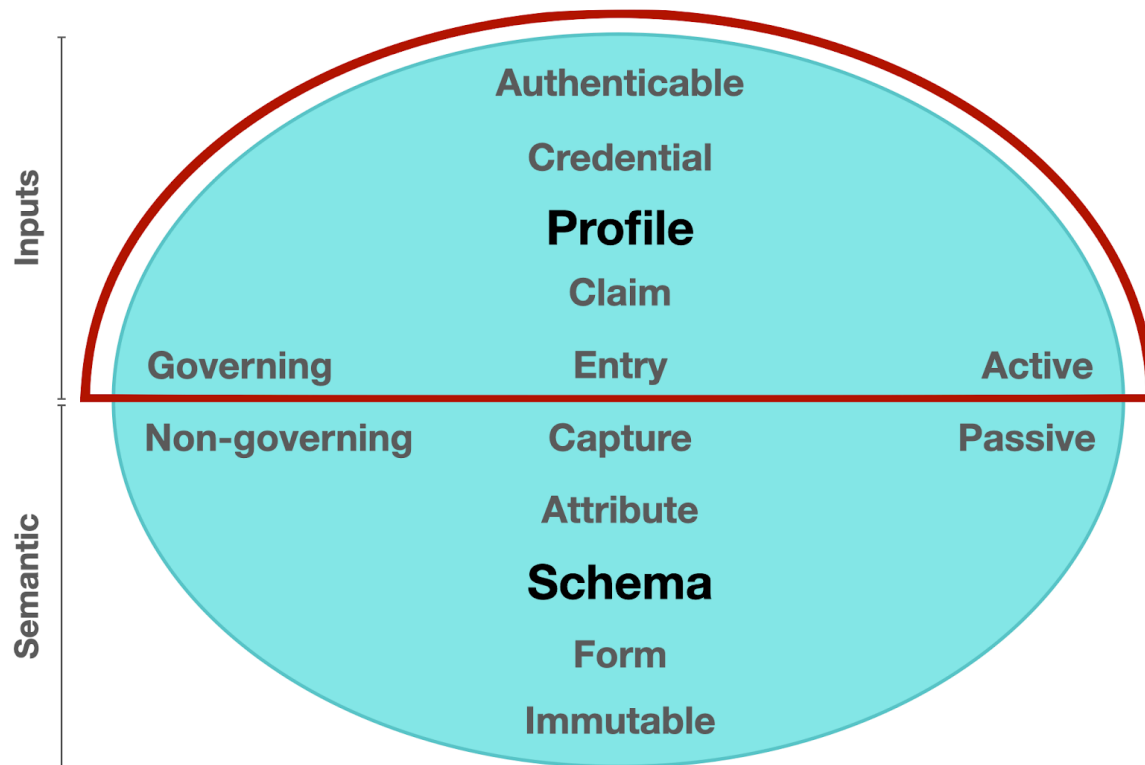
Other WG activities will include: (i.) creating template Requests for Proposal (RFPs); and (ii.) additional guidance to utility and service providers regarding implementations in that capacity.

This WG will be divided into *Inputs* and *Semantic* domain groups and may also organise Task Forces and Focus Groups to escalate the development of certain components if deemed appropriate by the majority of the WG members and in line with the overall mission of the ToIP Foundation.

## The Inputs Group

**Inputs domain [active]** / what is put in, taken in, or operated on by any process or system.

**Data entry** is defined as the process of inputting data into a computer using devices such as a keyboard, scanner, disk, sensor, or voice. In a decentralized network, data entry requires a signing key in order to establish that inputted data has come from an authenticable source. In the above component diagram, all elements and characteristics of data entry are depicted in the northern hemispherical *Inputs domain*.



Ref.:

<https://humancolossus.foundation/blog/cjzegoi58xgpfzwxryqlroy48dihwz>

## ISWG-I : Mission and scope

The mission of the Inputs group is to define a decentralized key management infrastructure that provides self-certifying identifier issuance underpinned by cryptographic one-way functions for Internet-scale deployment. The scope of this sub-group is to define specifications and best practices that bring cohesion to data entry processes and other *Inputs standards* throughout the ToIP stack, whether these standards are hosted at the Linux Foundation or external to it.

## ISWG-I : Description

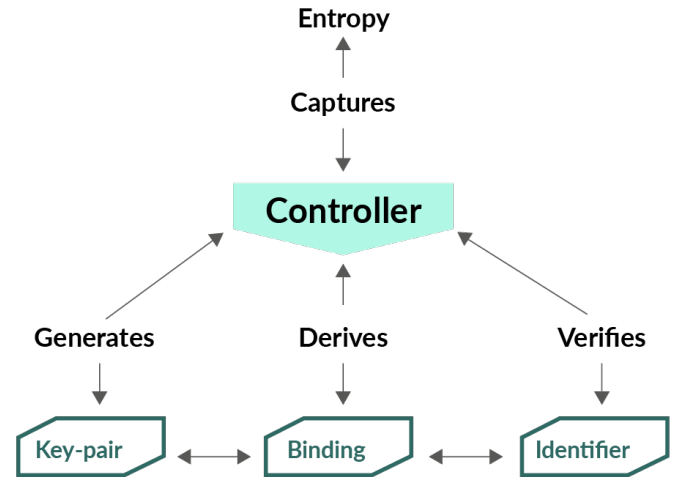
Key management refers to the management of cryptographic keys in a cryptosystem. This includes dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys. It includes cryptographic protocol design, key servers, user procedures, and other relevant protocols.

Successful key management is critical to the security of a cryptosystem. Developing and deploying the right key management infrastructure will ensure the highest level of security to enable tamper-resistant interactions between governing entities as autonomous peers in a digital system.

# ISWG-I : Key Event Receipt Infrastructure (KERI)

KERI is an architecture that offers information uniqueness from captured entropy by compiling the history of all uses or changes to the public/private key pair. This is achieved by universal self-certifying proofs of the binding between the self-certifying identifier (SCID) and the associated public/private key pairs. It is a truly decentralized key management solution offering the strongest possible levels of pseudonymity, ledger-less identity and separable identifier trust bases for all network participants.

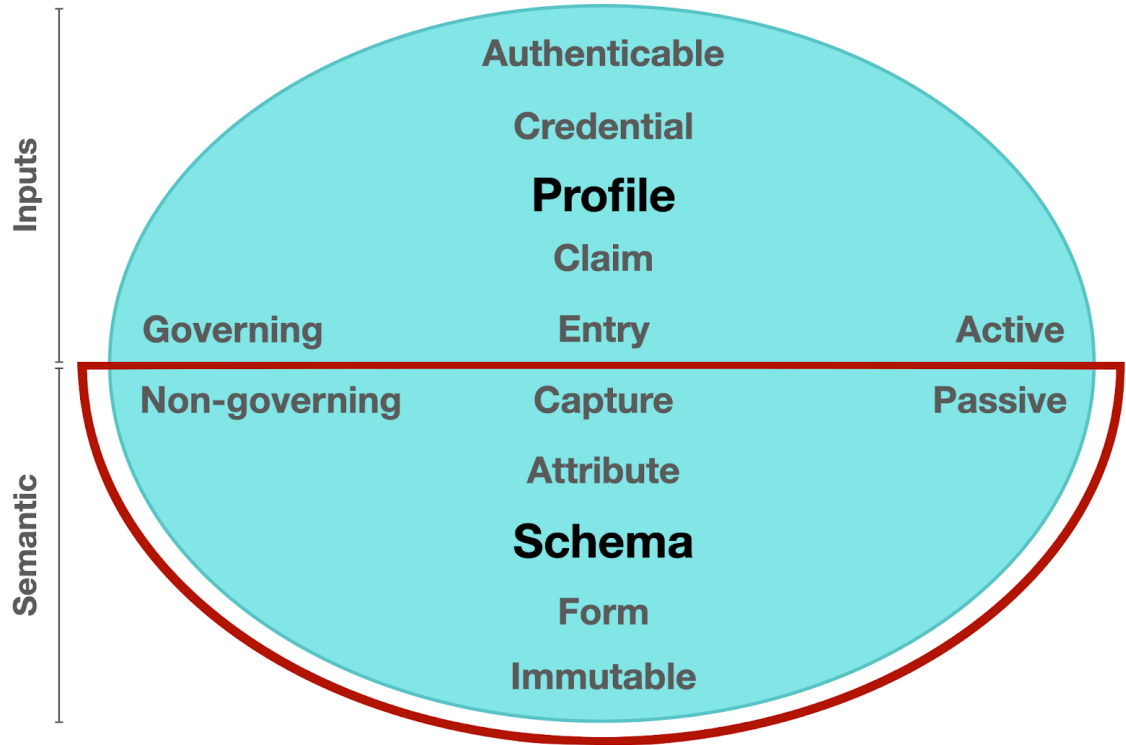
KERI is a secure overlay for an identity system where any digital representation of a governing entity can serve as an autonomous self-certifying root-of-trust. It is a solution that offers secure data control established via self-certifying pseudonymous identifiers. As a standardized global solution for data entry, KERI facilitates sapored data supply chains, enabling a record trail that accounts for the origin of data inputs operated on by any process or system.



# The Semantics Group

**Semantic domain** *[passive]* /  
the meaning and use of what is  
put in, taken in, or operated on  
by any process or system.

**Data capture** is defined as the process of collecting data electronically, allowing it to be stored, searched, or organized more efficiently. In a decentralized network, data capture requires the provision of immutable fields in order to capture and store collected data. In the above component diagram, all elements and characteristics of data capture are depicted in the southern hemispherical *Semantic domain*.



Ref.:

<https://humancolossus.foundation/blog/cjzegoi58xgpfzwxyrqlroy48dihwz>

## ISWG-S : Mission and scope

The mission of the Semantics group is to define a data capture architecture consisting of immutable schema bases and interoperable overlays for Internet-scale deployment. The scope of this sub-group is to define specifications and best practices that bring cohesion to data capture processes and other *Semantic standards* throughout the ToIP stack, whether these standards are hosted at the Linux Foundation or external to it.

## ISWG-S : Description

The post millennial generation has witnessed an explosion of captured data points which has sparked profound possibilities in both Artificial Intelligence (AI) and Internet of Things (IoT) solutions. This has spawned the collective realization that society's current technological infrastructure is simply not equipped to fully support de-identification or to entice corporations to break down internal data silos, streamline data harmonization processes and ultimately resolve worldwide data duplication and storage resource issues.

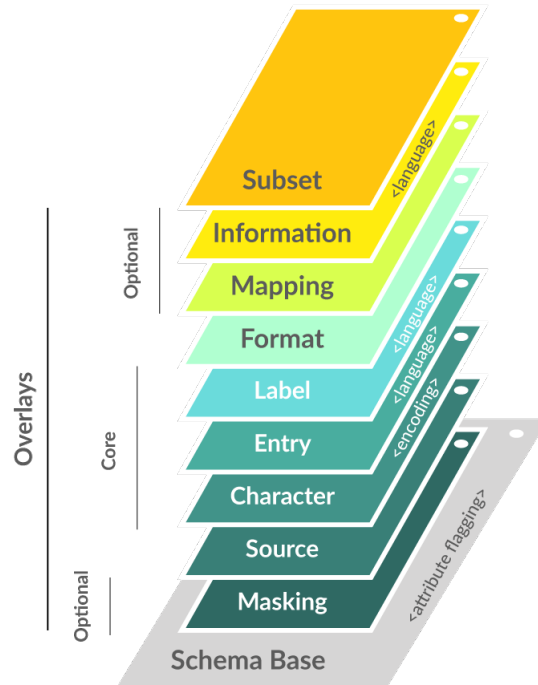
Developing and deploying the right data capture architecture will improve the quality of externally pooled data for future AI and IoT solutions.



# ISWG-S : Overlays Capture Architecture (OCA)

OCA is an architecture that presents a schema as a multi-dimensional object consisting of a stable *schema base* and interoperable *overlays*. Overlays are task-oriented linked data objects that provide additional extensions, coloration, and functionality to the schema base. This degree of object separation enables issuers to make custom edits to the overlays rather than to the schema base itself. In other words, multiple parties can interact with and contribute to the schema structure without having to change the schema base definition. With schema base definitions remaining stable and in their purest form, a common immutable base object is maintained throughout the capture process which enables data standardization..

OCA harmonizes data semantics. It is a global solution to semantic harmonization between data models and data representation formats. As a standardized global solution for data capture, OCA facilitates data language unification, promising to significantly enhance the ability to pool data more effectively for improved data science, statistics, analytics and other meaningful services.



## Proposed wiki structure for ISWG?

- › Inputs and Semantics WG
  - › Inputs Domain
  - › Semantic Domain
  - › Vertical Focus
  - › Horizontal Focus
  - › Meetings
  - › Glossary

Ref.:

<https://docs.google.com/document/d/1Mcettp8iMjRKUKdxJzwiGEw0PnGqtHFDDfsXxOpH5cQ/edit>

# Linking identifiers: Requirements and characteristics (10 mins)

Presented by: P.Knowles

<https://wiki.trustoverip.org/display/HOME/Passive+Identifiers>

## Passive identifiers

**Data capture** requires the provision of immutable fields in order to capture and store collected data. Immutable capture items are identified by *passive identifiers*.

| State         | Governing  | Non-governing                |
|---------------|--|------------------------------|
| Authenticable | Active   | Passive controlled by active |
| Immutable     | Active controlled by passive<br><i>(This state cannot exist)</i> | Passive                      |

Table: A hash grid table describing the different states of [active and passive identifiers](#). The two states of passive identifiers are highlighted.

## What is a Passive identifier?

An immutable identifier used to identify a non-governing entity, an inanimate object or a static data input. A passive identifier can either be (1) controlled by an *active identifier* or (2) not controlled.

### (i) **Controlled passive identifier** (*p/a-linkage*)

In general, passive identifiers for non-human resources do not need to be controlled. However, as soon as you have any need to express ownership, control, or management of that resource, you need to relate it to an active identifier. An *active identifier* identifies an entity that has the capacity to govern.

### (ii) **Uncontrolled passive identifier**

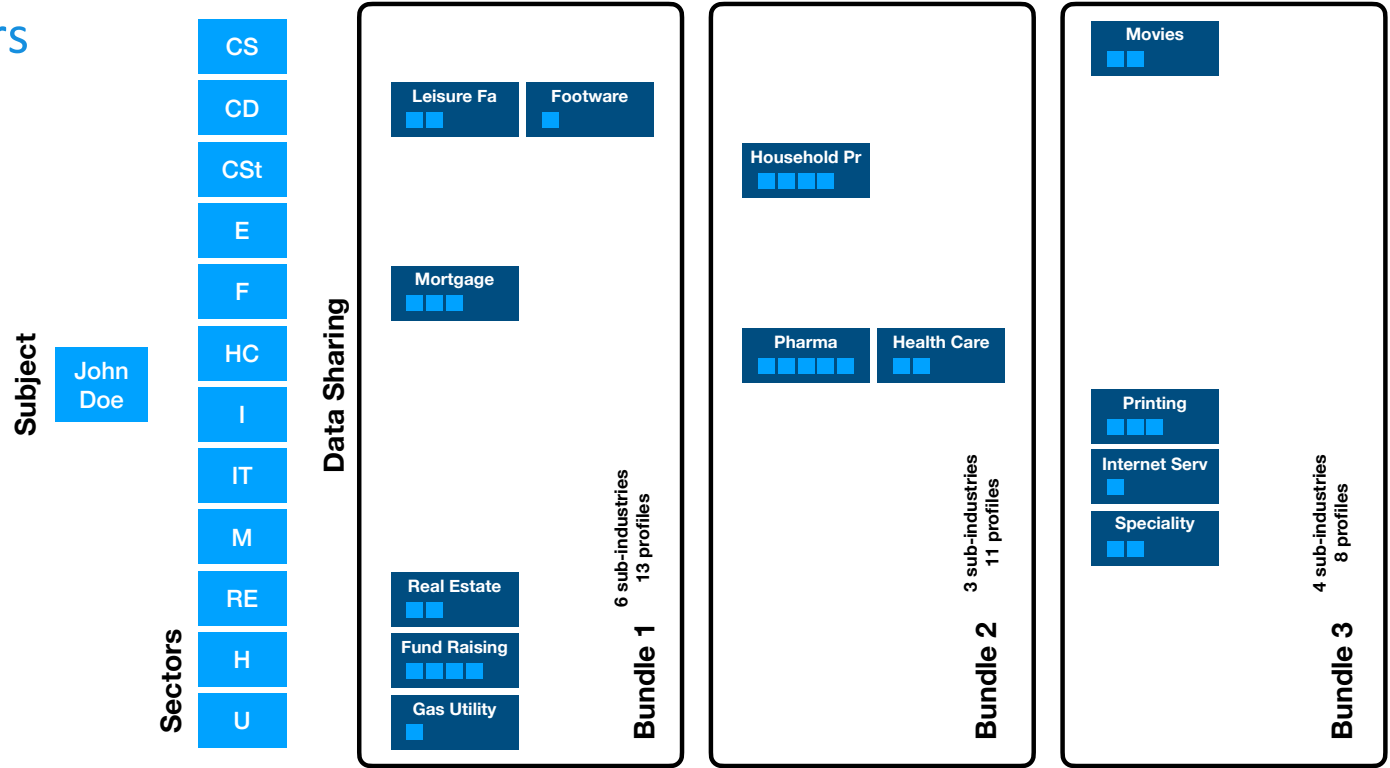
An immutable identifier that does not require any form of ownership, control, or management.

# What is a Linking identifier?

## **Linking identifier** (*p/p-linkage*)

An identifier that has an association with a cryptographic hash of digital content that can be used for linking information across a number of objects, applications and/or systems. A linking identifier can be referenced in multiple locations and, as such, changing any single reference of the linking identifier should propagate throughout the daisy chain. As a linking identifier tends to be governed, this threading property works well for data revocation where a governing entity has the capability of revoking all data associated with the linking identifier.

# Linking identifiers



A visual on what a linking identifier needs to achieve. In the diagram, there is one subject ('John Doe') with three consented data bundles. Each bundle includes a number of profiles. For each bundle, a linking identifier is needed as a thread to knit the profiles together. One linking identifier per consented bundle.

# GitHub Projects

## (15 mins)

Presented by: S.Milstein

<https://docs.github.com/en/free-pro-team@latest/github/managing-your-work-on-github/about-project-boards>

<https://github.com/features/project-management/>



# GitHub Projects

## About project boards

Project boards on GitHub help you organize and prioritize your work. You can create project boards for specific feature work, comprehensive roadmaps, or even release checklists. With project boards, you have the flexibility to create customized workflows that suit your needs.

Ref.: <https://docs.github.com/en/free-pro-team@latest/github/managing-your-work-on-github/about-project-boards>



## Project management, made simple

On GitHub, project managers and developers coordinate, track, and update their work in one place, so projects stay transparent and on schedule.

Ref.: <https://github.com/features/project-management/>

# Logistics and miscellaneous (5 mins)

<https://wiki.trustoverip.org/display/HOME/2020-11-10+Weekly+Meeting>

## News from the Operations Team

### **Nick Hayfack**

*(Semantics WG representative on the ToIP Operations Team)*

The purpose of the Operations Team is to create a small group of ToIP members who will share information on the workplans of our WGs, help ensure that draft deliverables are advancing as intended through the stages of the ToIP workflow, resolve any bottlenecks that arise around decision-making/approvals and discuss issues such as (for example) introducing firmer parameters for the creation of Taskforces under all WGs.

The Operations Team will not be directing or otherwise interfering with the development of content and deliverables in the WGs themselves.

## Leadership positions

- › Semantics WG Chair
  - › **Paul Knowles** (Human Colossus Foundation)
- › Semantics WG Vice-chair
  - › **John Wunderlich** (JLINC Labs)
- › Operations Team Group Representative
  - › **Nick Nayfack** (Team Ikigai)
- › We can periodically rotate chairs as needed
- › Volunteer via the meeting page at ...
  - › <https://wiki.trustoverip.org/display/HOME/2020-11-17+Weekly+Meeting>

## Meeting schedule

- › **OCA-FHIR FG** weekly meeting
  - › Thursday, **November 19th** @ 08:00 US PT / 17.00 CET
  - › Zoom link: <https://zoom.us/j/93406719136?pwd=SUozZHBQM0N5TUhYMhJqL0ZQM3I3Zz09>
- › **Semantics Domain WG** weekly meeting
  - › Tuesday, **November 24th** @ 09:00 US PT / 18.00 CET
  - › Zoom link: <https://zoom.us/j/93406719136?pwd=SUozZHBQM0N5TUhYMhJqL0ZQM3I3Zz09>
- › **Notice & Consent TF** bi-weekly meeting
  - › Thursday, **November 26th** @ 08:30 US PT / 17.30 CET
  - › Zoom link: <https://zoom.us/j/92346573961?pwd=RmZHNnQxS2Iya3NCMHZTVXYra3Rrdz09>



# Closing Q & A

# 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](mailto:legal@linuxfoundation.org) with any questions about The Linux Foundation's policies or the notices set forth on this slide.