

The background features a dark teal color with numerous thin, glowing teal lines that curve upwards from the bottom right towards the top left. These lines are punctuated by small, bright teal dots, creating a sense of depth and movement. The overall effect is reminiscent of a digital network or data flow.

LF DECENTRALIZED TRUST

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 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.

To provide a robust, common set of standard and complete architecture for internet-scale digital trust.

We focus on BOTH...

Interoperability and cryptographic verifiability at the machine layers

Human accountability at the legal, business, and social layers



member

OLF DECENTRALIZED TRUST

webinar

Verifiable Authenticity: How Trust Over IP is Answering the Threat of AI Deep Fakes



Judith Fleenor
Director of Strategic
Engagement - Trust Over IP



Drummond Reed
Director of Trust
Services - Gen



Wenjing Chu
Senior Director of Technology Strategy
- Futurewei Technologies, Inc



Karla McKenna
Managing Director/Head of
Standards - GLEIF

Date: November 13

Time: 10AM PT/1 PM ET/7PM CET



TRUST
Over IP

A deepfake crisis

Has been a long time coming
& has only just begun

IT SEEMED LIKE just another video call. Earlier this year, a finance worker based in Hong Kong for Arup, a British engineering firm, logged in for what he thought was a routine team meeting. On the screen, he saw several colleagues, including the firm's chief financial officer, who instructed him to transfer \$26m to five different bank accounts. He complied. But the man on the call was not Arup's CFO: it was a deepfake.

It was one of the costliest deepfake scams reported globally. Such scams are increasingly common. Deepfake technology, which manipulates images and video using artificial intelligence (AI), has become increasingly realistic. It is rapidly being adopted by transnational criminals mostly based in South-East Asia, now the epicentre of online scams targeting people around the world. Victims in East and South-East Asia lost up to \$37bn from online scams of all sorts in 2023, according to a new report from the United Nations Office on Drugs and Crime, the first time that it has come up with an estimate. According to the United States Institute for Peace, a think-tank in Washington, Cambodia's online scam industry makes more than \$12.5bn each year, equivalent to around half the country's formal GDP.

The old tools aren't working

&
both detection software and
watermarks can be defeated.

Suck up to your fake CEO

The deepfake scam explosion has only just begun



A deepfake of Lee Hsien Loong PHOTOGRAPH: FACEBOOK

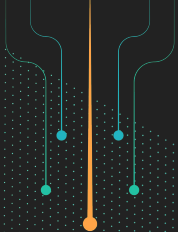
Online scam is being industrialized

Cambodia, a country of more than 16 m people, has a scam industry the size of almost half of its GDP

Many AI researchers think fakes will become undetectable

Both detection software and watermarks can be defeated





Verifiable Authenticity is the
foundation to truly answer
this threat

**And it should be built in a principled
way—like the IETF build the Internet.**



Since we are
defining an
architecture for
digital trust, of
course we need
technology...



Technology

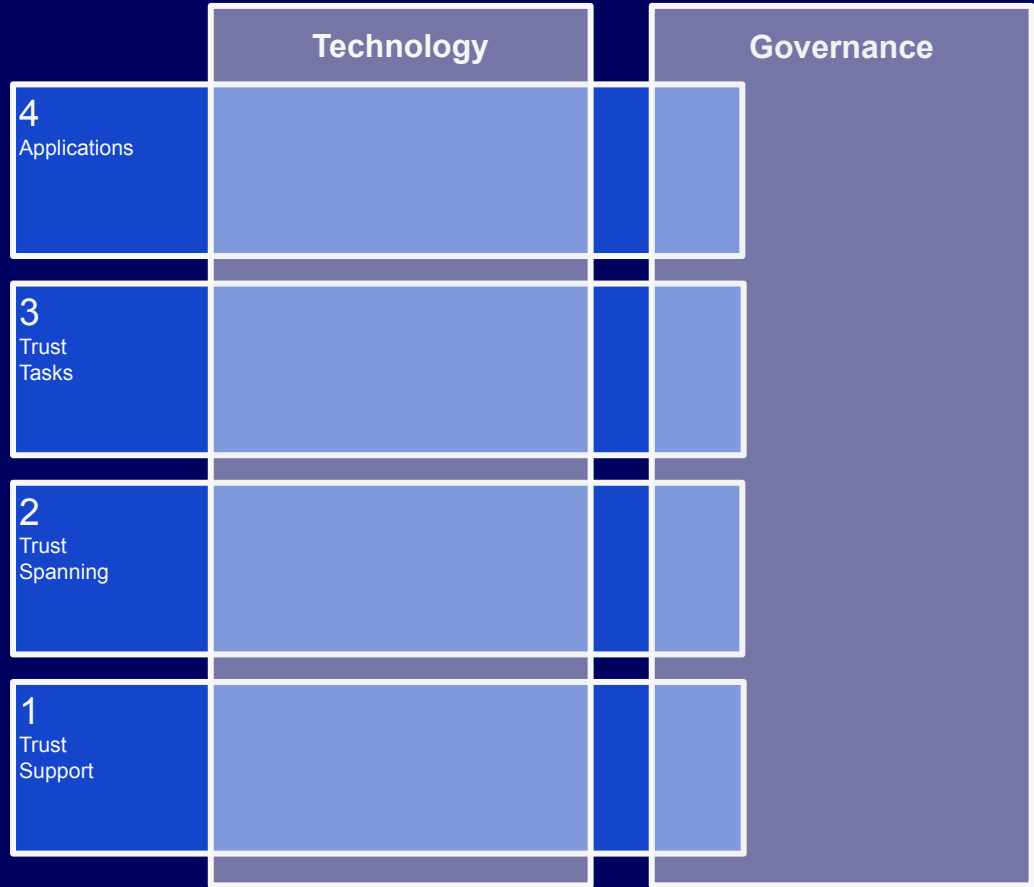
Technology

Governance

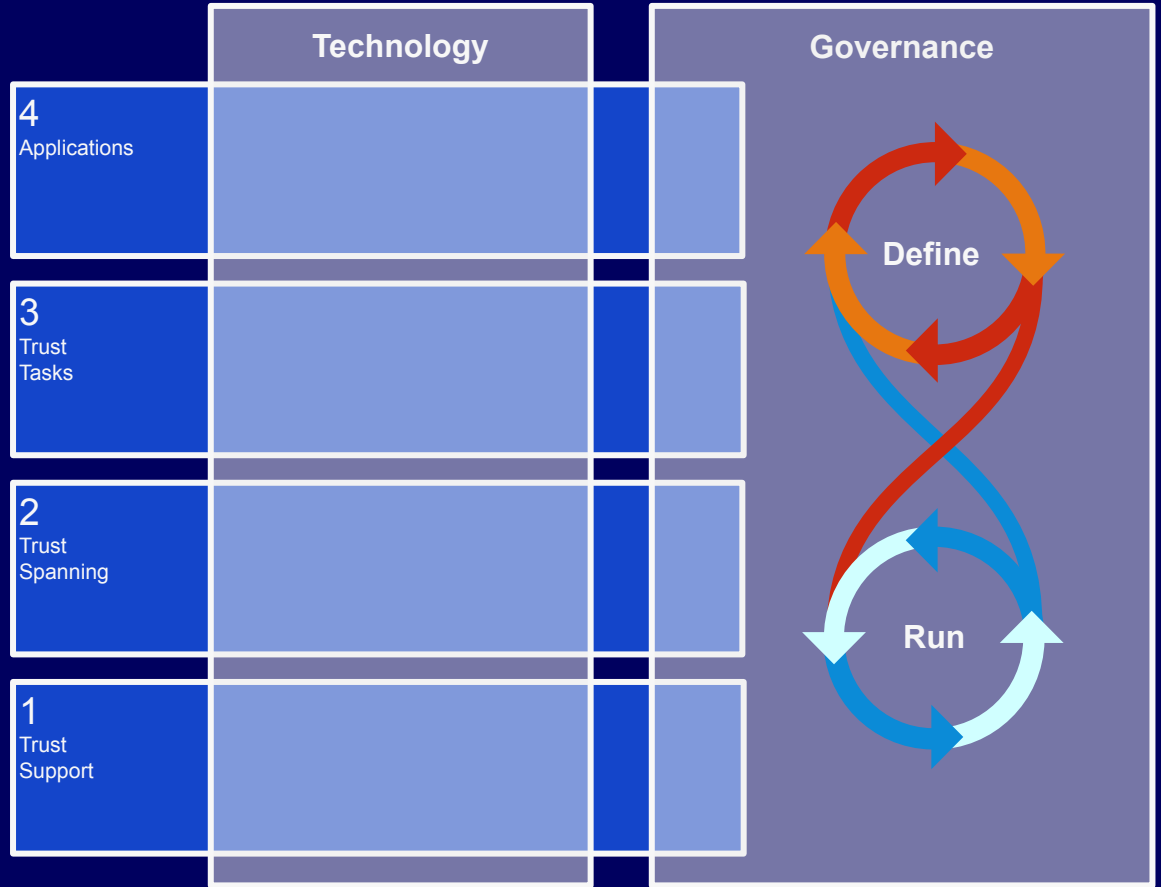
But technology
alone cannot
produce trust.

That only comes
with human
governance.

ToIP follows the same 4 layer stack as the Internet — only it integrates governance at each layer.

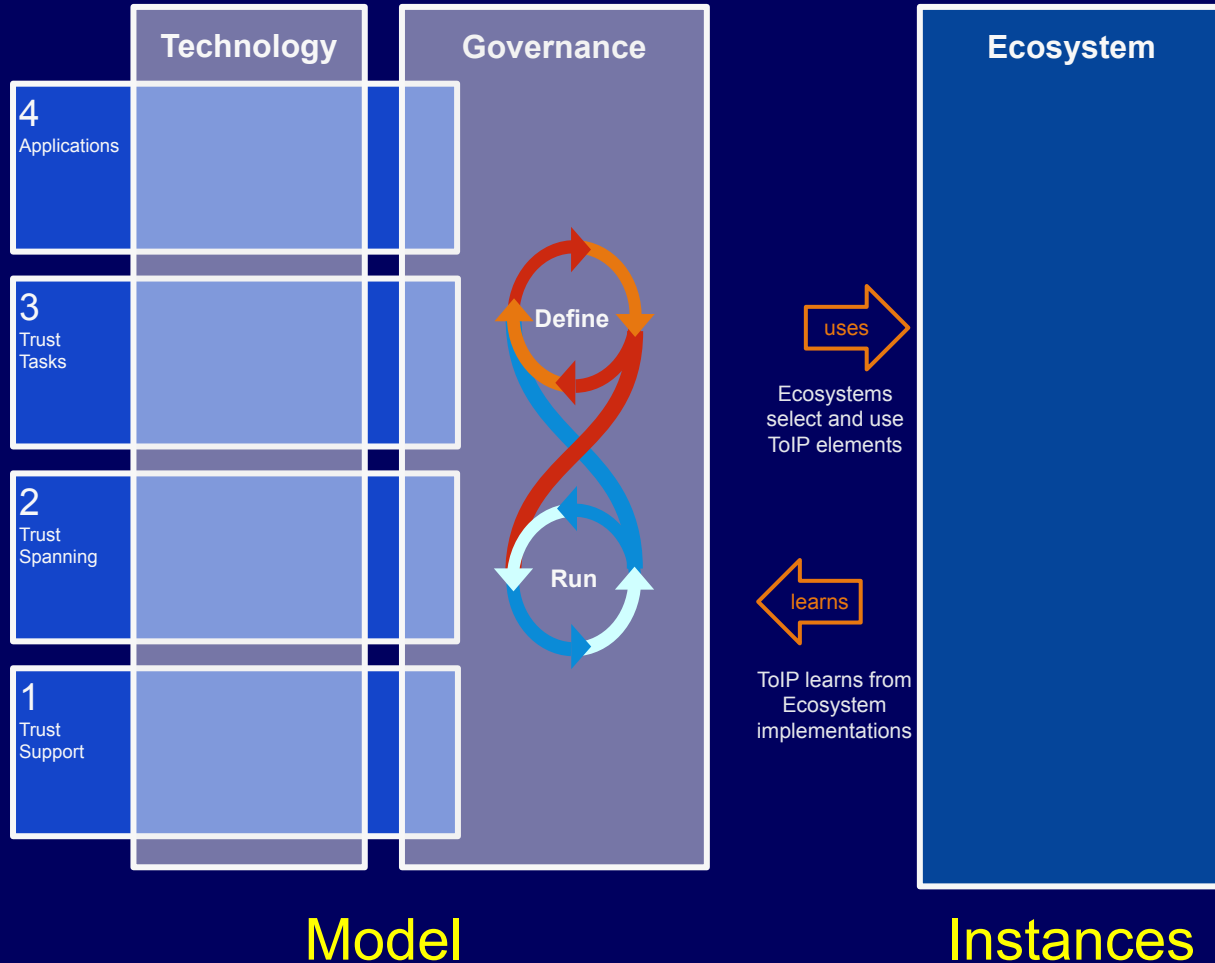


Governance is a living process—it evolves through define, run, and redefine cycles.

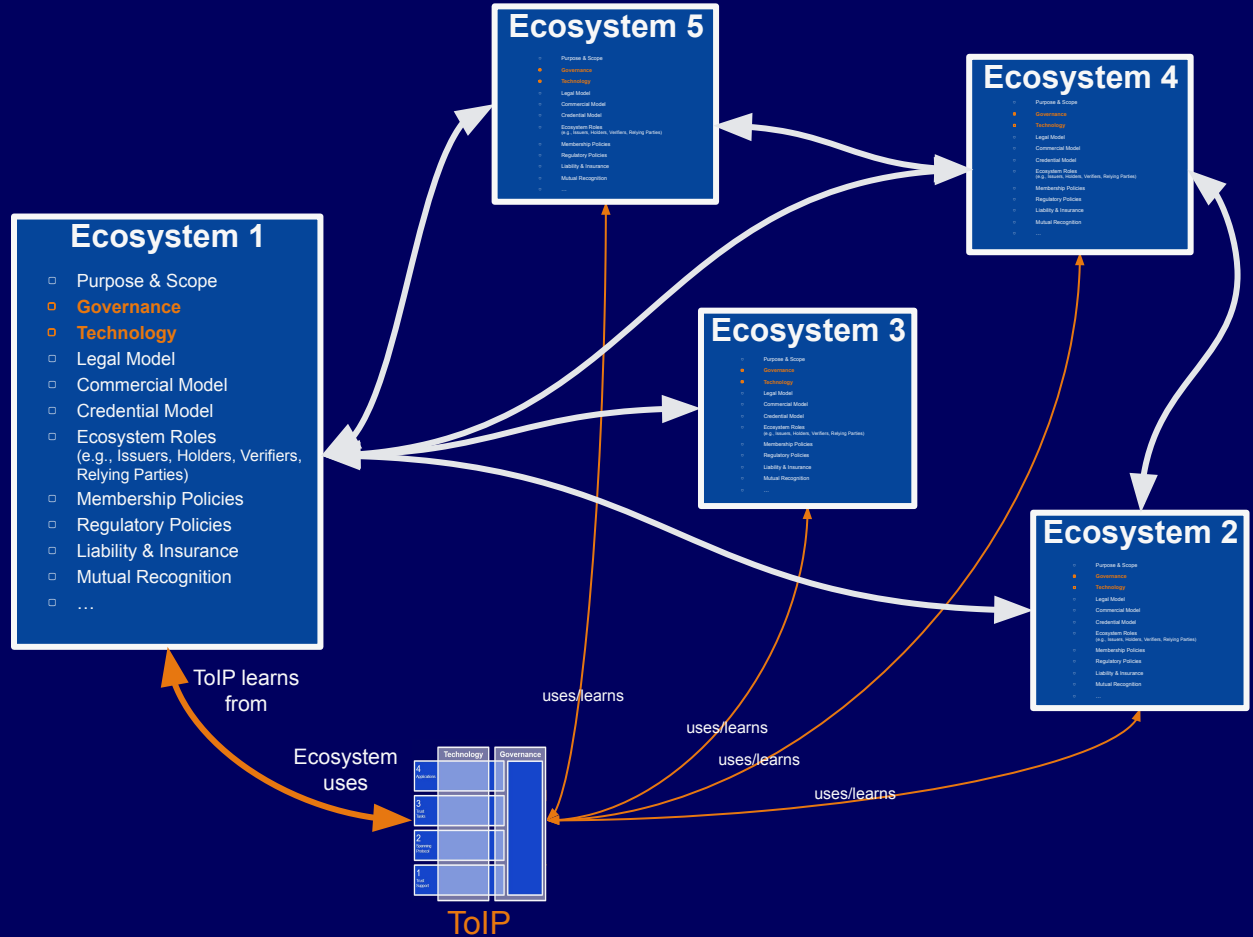


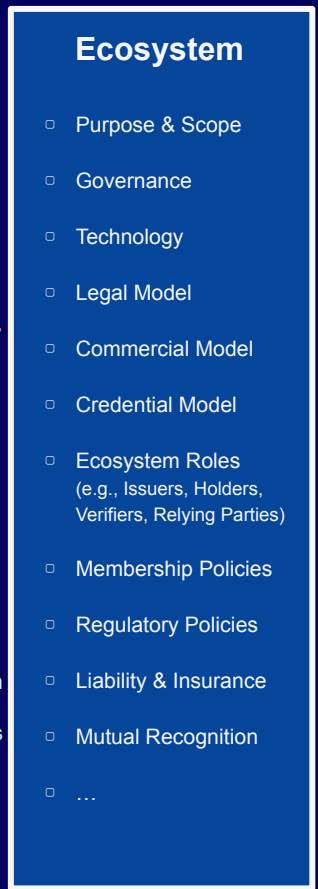
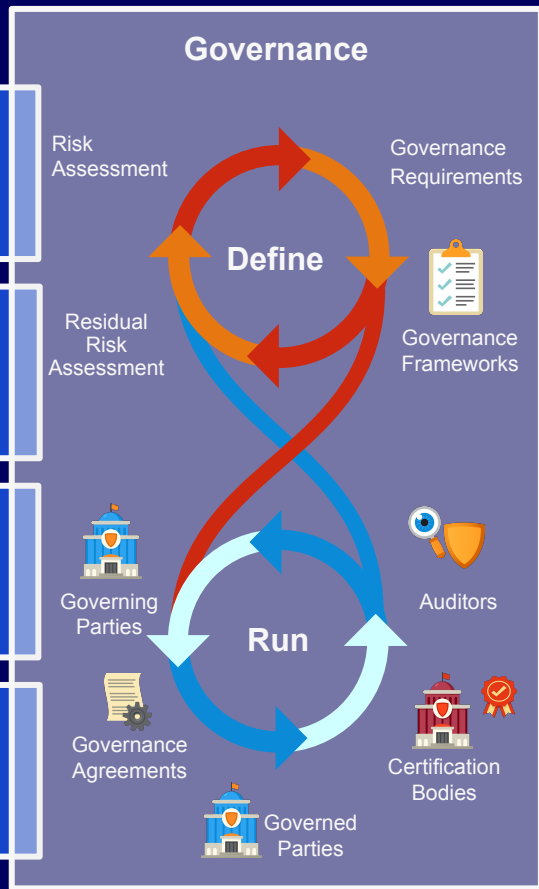
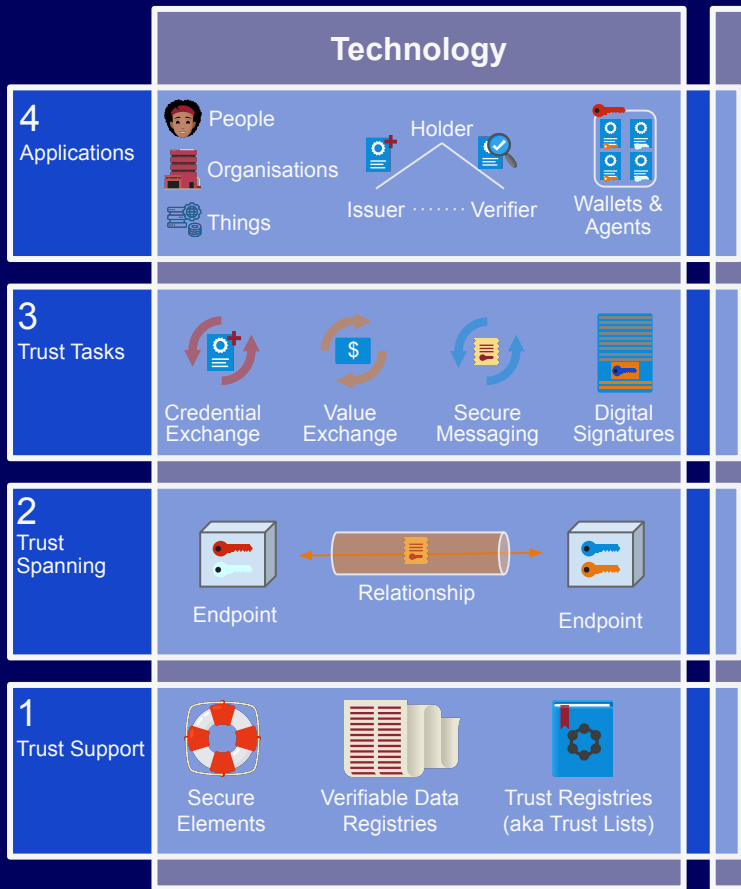
ToIP defines the **model**.

Digital trust ecosystems define **instances** of this model.



The goal of the ToIP stack is to enable a world of **interconnected & interoperable** digital trust ecosystems.





uses

Ecosystems select and use ToIP elements

uses

Ecosystems use other standards and frameworks

learns

ToIP learns from Ecosystem implementations

recognises

Ecosystems recognise other Ecosystems

ToIP Model
Span of Control

Ecosystem Instance
Span of Control

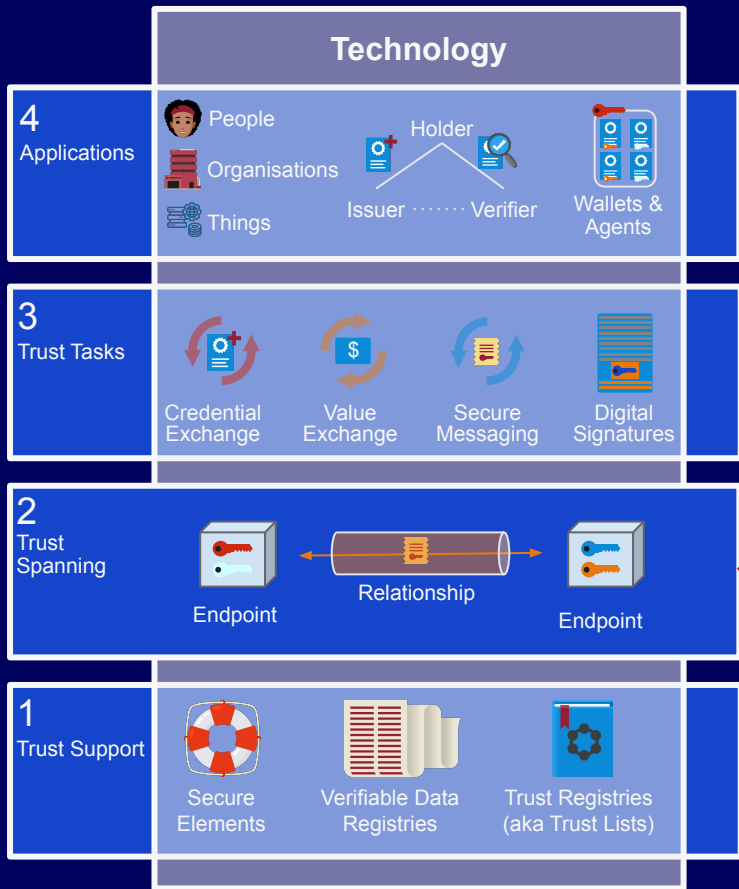
We have also created the **ToIP Glossary** to enable interoperability of terminology across digital trust projects & ecosystems.

The screenshot shows a web browser at the URL `glossary.trustoverip.org/#terms-and-definitions`. The page features a 'Table of Contents' sidebar on the left with seven items, where '7. Terms and Definitions' is selected. The main content area is titled '# 7. Terms and Definitions' and includes a sub-header '- There are 504 terms -'. Below this is a navigation bar with circular buttons for letters A through Z. The first three terms are visible:

- # AAL** [edit] [delete] [help] [up] See: [authenticator assurance level](#).
- # ABAC** [edit] [delete] [help] [up] See: [attribute-based access control](#).
- # acceptance network** [edit] [delete] [help] [up] A [trust network](#) designed to facilitate [acceptance](#) of [verifiable data](#) for its members.
- # acceptance** [edit] [delete] [help] [up] The [action](#) of a [party](#) receiving any form of [verifiable data](#) and using it to make a [trust decision](#). See also: [acceptance network](#).

glossary.trustoverip.org

Trust Spanning Protocol



TSP is a protocol design explicitly to serve as a universal spanning layer for digital trust relationships between any two parties—in the same way that IP serves as a spanning layer for data packets between to local area networks.

Layer 4 — Trust Applications

Other Trust Tasks

Query Trust Registry	Consent	Delegate	Sign	Vote	...
----------------------	---------	----------	------	------	-----

Value Exchange

Pay	Layaway	Bid	Stake	...
-----	---------	-----	-------	-----

Credential Exchange

Issue Credential	Present Proof	Revoke Credential	Bind Biometric
------------------	---------------	-------------------	----------------

Message Transfer
(e.g., SMTP, DIDComm)

Trusted Messaging

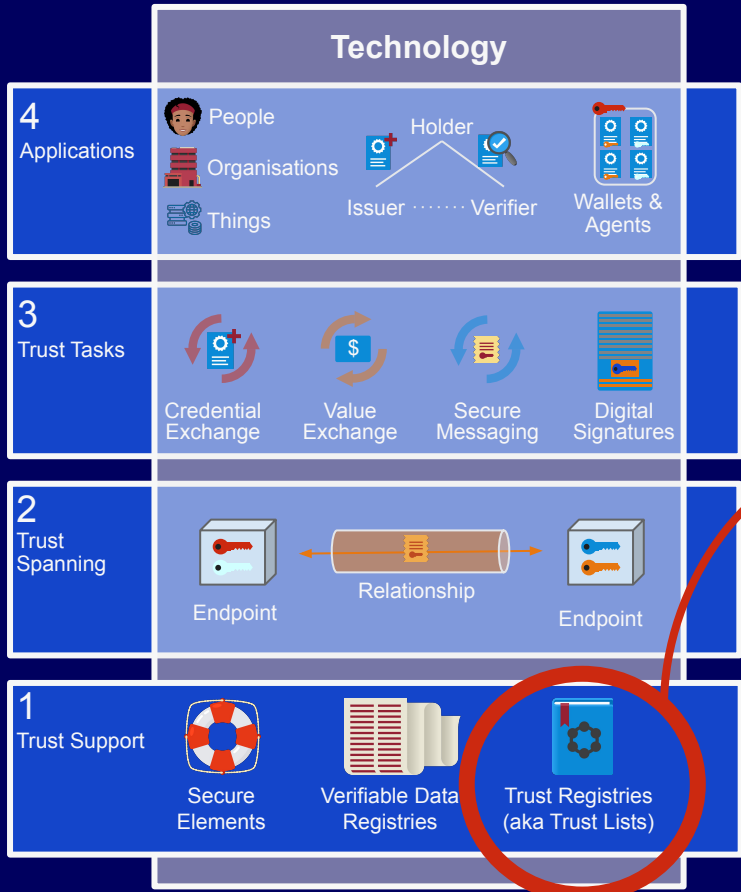
Trusted Data Sharing

State Transfer
(e.g., HTTPS, DWN)

Verifiable Authenticity, Confidentiality, & Metadata Privacy

Layer 2 — Trust Spanning

Layer 1 — Trust Support



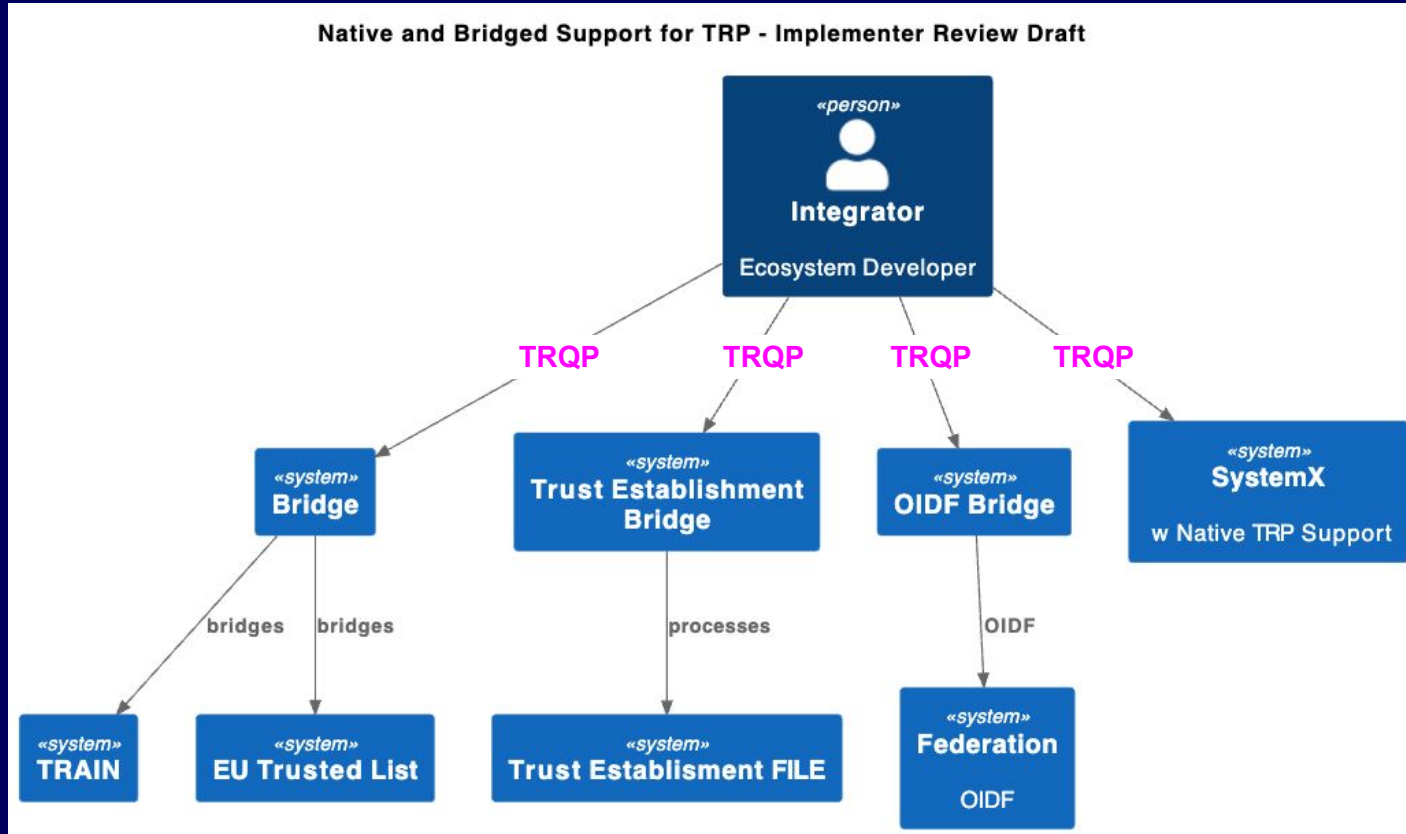
Trust Registry Query Protocol

TRQP is a simple standard protocol to query for authoritative ecosystem verification data—a “DNS for trust”.

Does Entity X have Authorization Y under Governance Framework Z?

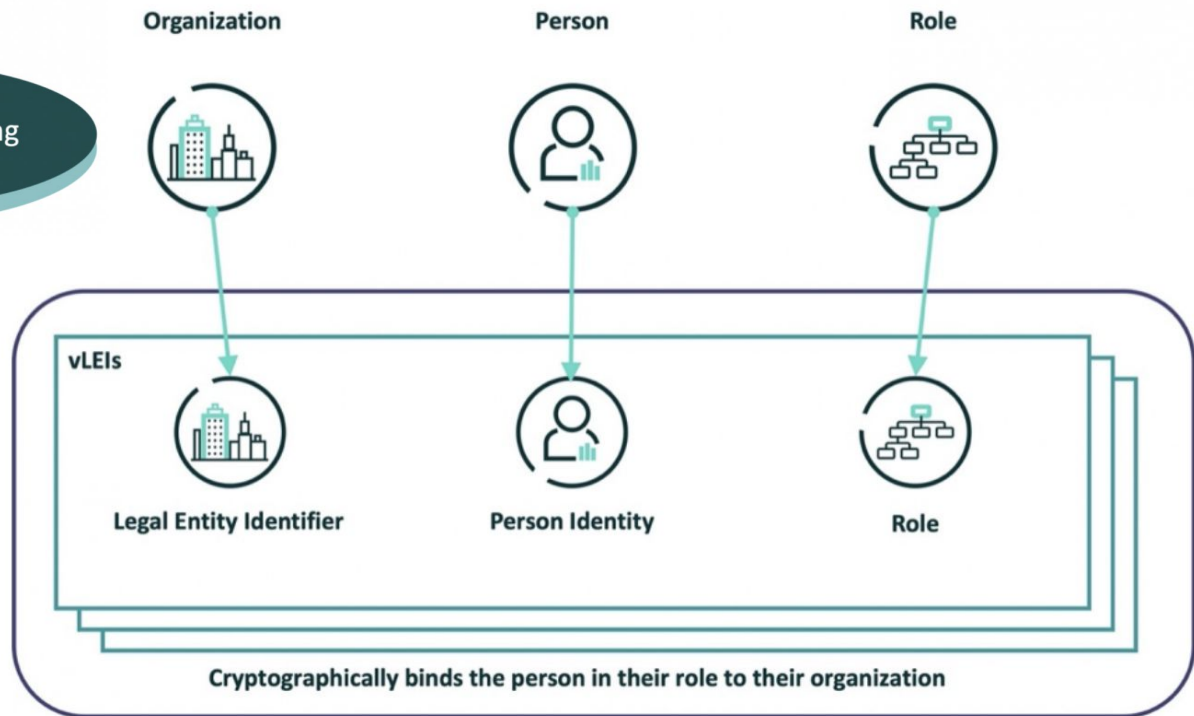
TRQP-enabled trust registries & trust lists enable trust decisions both within and across ecosystems.

TRQP can be adapted to talk to any authoritative source



The Governance Cycle







Questions?

ToIP Presenters



Judith Fleenor

ToIP Director of Strategic Engagement
judith@trustoverip.org



Drummond Reed

Gen Digital
Drummond.Reed@gendigital.com Karla.Mckenna@gleif.org



Karla McKenna

GLEIF
Karla.Mckenna@gleif.org



Wenjing Chu

Furturewei Technologies
wchu@futurewei.com

Contact

LFD T Leadership



Daniela Barbosa

Executive Director

dbarbosa@linuxfoundation.org



Julian Gordon

VP, Asia Pacific and Middle East

jgordan@linuxfoundation.org



Karen Ottoni

Sr. Director of Ecosystem
& Strategic Initiatives

kottoni@linuxfoundation.org



Hart Montgomery

Chief Technical Officer

hmontgomery@linuxfoundation.org



David Boswell

Sr. Director Community Architect

dboswell@linuxfoundation.org