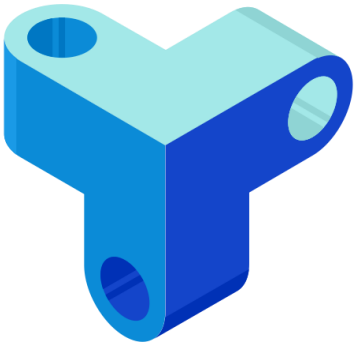


TRUST Over IP FOUNDATION

Do You Trust Me?

November 10, 2021
APPROVED EFWG DRAFT

The mission of the Trust over IP (ToIP) Foundation is to define a complete architecture for Internet-scale digital trust that combines cryptographic assurance at the machine layer with human accountability at the business, legal, and social layers. Founded in May 2020 as a non-profit hosted by the Linux Foundation, the ToIP Foundation has over 300 organizational and 100 individual members from around the world.

Please see the end page for licensing information and how to get involved with the Trust Over IP Foundation.

Document Information

Acknowledgements

The authors and contributors would like to acknowledge the Trust Over IP Foundation community for their ongoing insights, ideals and principles. This paper is a reflection of our community.

Author

Karen J Hand — PhD, Precision Strategic Solutions

Contributors

Chris Ingrao,
Drummond Reed, Evernym
Jim StClair,
Judith Fleenor, Trust Over IP Foundation
Karl Kneiss, IdRamp
M. Oskar van Deventer
Rieks Joosten,
Scott Perry, Scott S. Perry CPA, PLLC
Sankarshan Mukhopadhyay, Dhiway Networks
Wenjing Chu, Futurewei
P. A. Subrahmanyam, CyberKnowledge

Revision History

Version	Date Approved	Revisions
1.0	23 September 2021	Draft EFWG Approval
1.1	05 November 2021	Final Draft EFWG Approval

Terms of Use

Do You Trust Me?

Human society is built on trust. There is implicit and explicit trust in every transaction; whether human, technical, or digital. **Do you trust me? Should you trust me?**

What Does Trust Mean?

Trust is defined by the context, outcome, and significance of our experiences. Thus, trust is dynamic. The conundrum of 'to trust' or 'not to trust' is never binary; it is fluid, changing over time and circumstance. Rousseau et al (1998)[1], challenged by the inconsistent conceptions of interpersonal and organizational trust across disciplines, leveraged the work of Mayer et al (1995[2]) to define a shared understanding of trust as "a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another".

Hofstede (2007)[3] studied the implications of trust (as defined by Rousseau et al, 1998[1]) and transparency in supply netchains and found trust builds gradually through experience; for example, a supplier who voluntarily (as opposed to obligatory) warns a buyer of a lapse in supply. More recently, van Prooijen et al (2022)[4] found the growing trend towards citizen suspicion (and conspiracy theory) of institutions reduces trust between strangers, collaborations within groups, and prosocial behavior; ultimately, eroding the fabric of society. These studies illustrate how trust grows over time and experience and distrust is a result of suspicion or belief in one's feelings.

For humans, trust is an integral neurological component, a survival instinct that allows us to work together for common goals, build healthy relationships, a healthy society and be innovative in our approach to everyday challenges.

What Digital Society Has Brought - Complexity

Today, digital transformation—characterized by the ongoing evolution of organizations through the increasingly interconnected nature of our society, business, and technology—is delivering profound and disruptive impacts by enabling innovative business opportunities

[1] Rousseau, D.M., Sitkin, S.B., Burt, R., Camerer, C. (1998). Not so different after all: a cross-discipline view of trust. Academy of Management Review, 23(3), 393-404.

[2] Mayer, Roger C., James H. Davis and F. David Schoorman, "An Integrative Model of Organizational Trust", The Academy of Management Review, vol, 20, no. 3, 1995, p. 712, https://doi.org/10.2307/258792.

3 Hofstede, Gert Jan. (2007). Trust and Transparency in Supply Netchains: A Contradiction? Supply Chain Management: The New Era of Collaboration and Competition.

[4] Jan-Willem van Prooijen, Giuliana Spadaro, Haiyan Wang. (2022). Suspicion of institutions: How distrust and conspiracy theories deteriorate social relationships. Current Opinion in Psychology, 43: 65 – 69. https://doi.org/10.1016/j.copsyc.2021.06.013.

and equally innovative solutions to challenges related to our environment, health, productivity, and resource allocation.

One can now imagine a world – a digital sustainable world - where data flows freely. A global society where decisions affecting our society, and our planet, are no longer reactive. In this society, insights are achieved through synergies that are not even imaginable to us today. Bound tightly to the Sustainable Development Goals (SDGs) adopted by all United Nations Member States in 2015, is the idea first proposed by Japan of *Society 5.0*, described as "a super-smart society, and one that will serve as a road map for the rest of the world" (Minevich, 2019)[5]. To realize the vision of a smart society one must address the challenges of human-technology trust as well as the complexities of human trust in human-centric societies, whether digital or not.

How Do We Cope with This New Reality?

How do we come to a shared understanding of trust in this ever evolving, complex ecosystem of citizens, consumers, and organizations (for-profit, not-for-profit, research, non-governmental and governmental) with competition at the local, regional, provincial, national, and global levels? How do we become knowledgeable enough to accept vulnerability with or without knowing the intentions or behaviours of others?

The European Commission recently identified the trust gap between people and technology as a significant risk to the European Union—with potential to negatively impact both consumers and businesses. As a result, it has implemented a number of core initiatives (or pillars) under the European Digital Strategy[6] to mitigate the risks associated with the trust gap; including a framework for trusted and secured digital identities and digital identity wallet for EU citizens.[7]

We need to trust the digital technologies that will enable *Society 5.0*, but more importantly the digital relationships within *Society 5.0*; human-to-human, human-to-machine, and machine-to-machine. We need to make decisions, as simple as agreeing to a social connection or agreeing to a business arrangement with potential to impact our well-being. Every decision requires measurable proof of authenticity, verification of who you are, expectations of behaviour, and the information necessary to move forward - in other words: "Trust but Verify".

[5] https://techcrunch.com/2019/02/02/japans-society-5-0-initiative-is-a-roadmap-for-todays-entrepreneurs/. Accessed July 2021.
[6] https://ec.europa.eu/commission/commissioners/2019-2024/vestager/announcements/trust-and-technology-new-digital-age_en
[7] https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

BUSINESS

How does one measure digital trust? The Edelman Trust Barometer 2020[8] argues that ethics (integrity, dependability, purpose) are three times more important to establish trust in a company than competence. This is an argument supported by Connelly et al (2015)[9], who found that integrity-based trust (i.e., motives, honesty, and character) were ten times more effective at reducing the cost of business over competence-based trust (i.e., technical skills, experience, and reliability).

The recent Edelman Trust Barometer 2021[10] found business is now expected to fill the trust void left by government institutions. In other words, CEOs are expected to be leaders on societal issues, rather than wait for governments to impose regulations, and are expected to hold themselves accountable to the public, not just boards of directors or stockholders. Businesses and governments now seek market advantage through brand trust, as seen in the current movement of organizations committing to a net zero carbon future.

All three studies underline the importance of digital trust as a determinant of business success and sustainability.

Further, there are significant consequences of distrust in business ecosystems. In a recent study exploring the use of innovative technologies (for example blockchain) to optimize global food supply chains (FSCs), Keogh et al (2020)[8] depict FSCs as a metaphoric "chain of trust", fundamental to the integrity of our food systems. The authors argue this "chain of trust" is under challenge due to the complexities of globalization, creating a food system where critical information is not available to consumers, with rising crises in food safety, authenticity, defense, and security. The result: growing debate over food supply chain integrity along with significant economic loss, estimated to be in the hundreds of billions.

In moving forward, business organizations and ecosystems need to establish digital trust to be successful and sustainable. They need to embrace the principle of "Trust but Verify".

Citizens

The World Economic Forum (WEF, 2021) recently published a report concerning the empowerment of human-centric data societies11; where the values, needs and expectations of people, groups, and communities defines the core tenet of how data is governed. The report notes human centricity demands humans as the logical point of integration that are actively engaged with the will and capacity to improve their lives with data interoperability

[8] https://www.edelman.com/trust/2020-trust-barometer. Accessed July 2021.
[9] Connelly, B.L, Crook, T.R., Combs, J.G., Ketchen, D.J, Aguinis, H. (2015). Competence- and integrity-based trust in interorganizational relationships: which matters more?. Journal of Management. https://doi.org/10.1177/0149206315596813
[10] https://www.edelman.com/trust/2021-trust-barometer. Accessed July, 2021.
[11] https://www.weforum.org/whitepapers/empowered-data-societies-a-human-centric-approach-to-data-relationships

across all technologies, policy and valuation models, with applicable and interoperable frameworks (both global and cross-cultural) as well as appropriate levels of responsibility and freedom, and risk and opportunities. The report illustrates the importance of policy in building trust in data relationships.

A 2018 report by the United Nations Department of Economic and Social Affairs (DESA)[12] predicts that by 2050, 2.5 billion people are expected to move into urban areas, feeding the growth of mega-cities. The report posits that sustainable urbanization will be a key determinant for successful urbanization, while identifying several challenges related to housing, transportation, energy systems, employment, education, and health care. The report urges governments to adopt integrated policies to improve the lives of both urban and rural citizens. As part of addressing this challenge, the EU has announced the European Digital Identity framework and use of the new European Digital Wallet, which will enable all citizens to access online services allowing them to oversee the sharing and control of their personal data[13].

This is an example of how these human-centric ideals are being embraced by the newly emerging digital society and digital economy. Other evidence is the growing number of citizen-centric governmental initiatives, such as the UN SDGs, the British Columbia Services Card,[14] and Ontario's digital identity program as part of Ontario Onwards – a COVID-19 action plan for a people-focused government[15] (and numerous smart city initiatives.

Certainly, the establishment of a human-centric digital society will need to address the trust gap between people and technology. More significantly, it will need to address the trust gap between people and institutions. According to the 2020 Edelman Trust Barometer[7], over half of respondents suspect societal leaders (i.e., those in government and business) of lies and misinformation; trust in all information sources is at a record low. The challenges are complex, the WEF 2021[11] report demonstrates for example the potentially far deeper implications and dynamics underlying a simple engagement with a public sector service.

For citizens, the consequences of distrust are continued lack of information, technology adoption hesitancy, and a growing inequality regarding access to our core needs: housing, transportation, energy systems, employment, education, and health care, and overall capacity to improve quality of life.

"Trust but Verify" is a core principle for the newly emerging digital society that will enable trustworthy and innovative approaches not just for proof of identity, but for unimpeachable, immutable proof of our attributes (health, education, finance) that define who we are and

[12] https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html. 2018 Revision of World Urbanization Prospects.
[13] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663
[14] https://www2.gov.bc.ca/gov/content/governments/government-id/bc-services-card
[15] https://www.ontario.ca/page/ontario-onwards-action-plan

directly impact our interaction with the digital and non-digital world. As basic as this sounds, the challenges with reliable and equitable records of identity continue to challenge citizens in every country and affect our basic right to be recognized.

Society

In his concluding remarks, Edelman (2021)[7] emphasized trust as the most important currency in lasting relationships between all institutions studied (non-governmental, governmental, business, media organizations and their various stakeholders). Particularly in times of turbulence and volatility, trust holds society together and every institution needs to play its part.

However, there is no direct line of sight to address the complexity of trust and inclusiveness, and no one size fits all. We often speak of using innovative technologies to enable trust (e.g., blockchain, distributed ledgers, data trusts); however, technology is a tool, not an objective. We need to understand where we are as a society, business, or citizen and where we want to go. Only then can we identify the technologies that will get us there.

Trust requires proof – "Trust but Verify". This will require every person, object, organization, machine, to possess an identity, a digital proof of "I am" and "This is me" – verified, unimpeachable, immutable, distributed, and trusted authentication.

Why the Trust Over IP Foundation?

"Trust but Verify" is a core tenet of The Trust over IP Foundation[16] (ToIP) community of individuals and member organizations participating in an independent project to define a complete architecture for Internet-scale digital trust that combines cryptographic verifiability at the machine layer and human accountability at the business, legal, and social layers.

The architecture is based on a triangle of trust between holders, issuers, and verifiers of digital credentials as shown below in Figure 1.

[16] https://trustoverip.org/. Accessed July 2021.

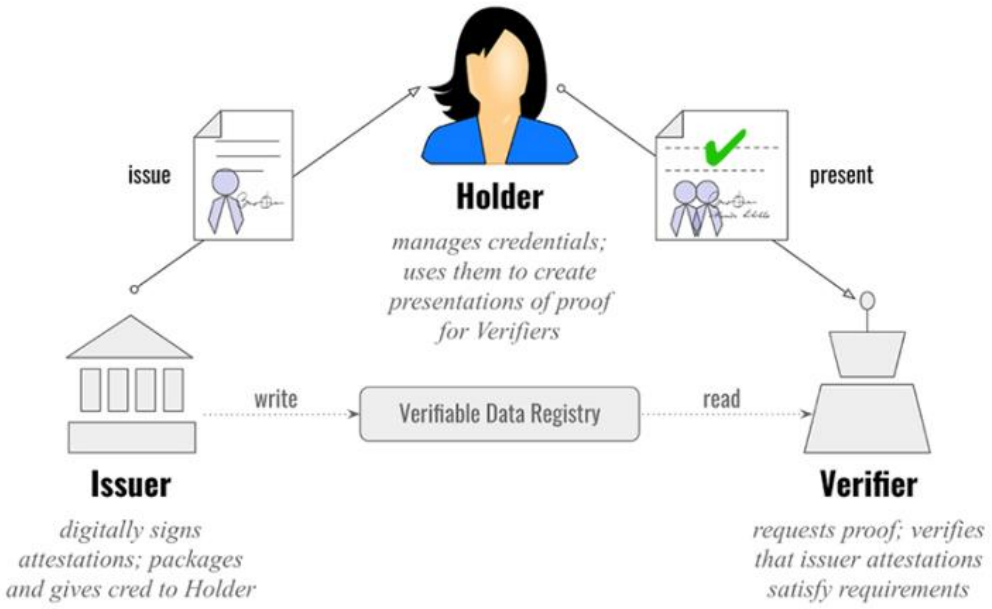


Figure 1: Triangle of trust architecture

Holders use a digital wallet to store tamper-proof personal information that has been issued to them in the form of digitally-signed credentials. Verifiers can then request a holder to present cryptographically verifiable proof of specific information from those credentials—proof that is only provided with the consent of the holder, and in the most privacy-preserving way. Within an ecosystem that uses such digital credentials—a *digital trust ecosystem*— the role of holder, issuer, and verifier can be performed by human as well as non-human actors, including IoT devices, machines, plants, or animals. Ecosystem members can assume multiple roles, depending on the transaction in question. Verified credentials can be simple (e.g., "I am a Holstein cow," or "I am nineteen years old"), specific (e.g., "Laboratory ABC analyzed this Sample on this Date with this Result"), or more complex as in the case of identity (e.g., digital passport, driver's license, diploma, or health status and information).

Quis Custodiet Ipsos Custodes?

"Who watches the watchmen?"[17] This is a critical question and core component of the ToIP digital trust architecture. This architecture includes two core components: 1) *governance frameworks* that specify the policies to which the members of a digital trust ecosystem agree to adhere, and 2) *trust registries* that enable anyone to verify which ecosystem members are authorized to perform what actions—for example, which issuers are authorized to issue what types of verifiable credentials; which verifiers are authorized to request what types of verifiable presentations; and under what conditions such credentials can be

[17] Moore, Alan, and Dave Gibbons. Watchmen. New York: Warner Books, 1987. Print.

revoked. Standardized public governance frameworks provide governance transparency between digital trust ecosystems.

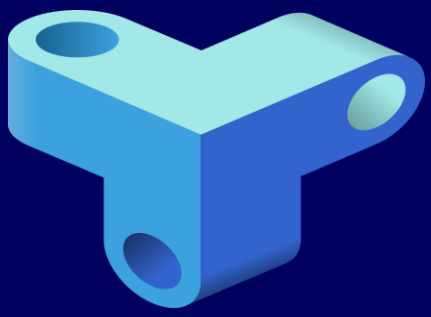
In Summary

Addressing the complex trust challenges brought about by digitization requires a complete architecture for Internet-scale digital trust that encompasses devices, individuals, and organizations. This is the solid foundation of trust we need if we are going to leverage collective intelligence and expertise to enable innovative business opportunities and solutions to societal challenges.

Should you trust me? Yes, you should – when supported by the "Trust but Verify" principles of ToIP digital trust architecture. This architecture has been developed from the ground up for the express purpose of enabling automated, dynamic, trusted transactions built on a balanced approach of secure, interoperable, open technology supported by rigorous and human-driven governance.

Do you trust me? That will always be a personal choice. ToIP is working to enable "Trust but Verify" transactions, providing organizations, governments, and communities of all sizes with the tools to build digital trust ecosystems.

No system or technology can ever provide an absolute guarantee and it is always your prerogative to say "No, I do not trust you". In the end the choice will be between progress and innovation or caution and maintaining the status quo. ToIP is a tool for innovation and progress in our digital society. We invite you to join us in forging a path together into the next stages of our evolving digital world.



TRUST Over IP FOUNDATION

The Trust Over IP Foundation (ToIP) is hosted by the Linux Foundation under its Joint Development Foundation legal structure. We produce a wide range of tools and deliverables organized into five categories:

- Specifications to be implemented in code
- Recommendations to be followed in practice
- Guides to be executed in operation
- White Papers to assist in decision making
- Glossaries to be incorporated in other documents

ToIP is a membership organization with three classes—Contributor, General, and Steering.

The work of the Foundation all takes place in Working Groups, within which there are Task Forces self-organized around specific interests. All ToIP members regardless of membership class may participate in all ToIP Working Groups and Task Forces.

When you join ToIP, you are joining a community of individuals and organizations committed to solving the toughest technical and human centric problems of digital trust. Your involvement will shape the future of how trust is managed across the Internet, in commerce, and throughout our digital lives. The benefits of joining our collaborative community are that together we can tackle issues that no single organization, governmental jurisdiction, or project ecosystem can solve by themselves. The results are lower costs for security, privacy, and compliance; dramatically improved customer experience, accelerated digital transformation, and simplified cross-system integration.

To learn more about the Trust Over IP Foundation please visit our website, https://trustoverip.org.