TRUST Over IP FOUNDATION

Practical Steps for Overcoming Human Harm Challenges in Digital Identity Ecosystems

Version 1.0
04 May 2023

This publicly available guide was approved by the ToIP Foundation Steering Committee on 24 May 2023.

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

Author

Author: Nicky Hickman - Come to the Edge Ltd

Contributors

Andrew Slack - SICPA

Revision History

Version	Date Approved	Revisions
1.0	24 May 2024	Initial Publication

Terms of Use

These materials are made available under and are subject to the Creative Commons Attribution 4.0 International license (http://creativecommons.org/licenses/by/4.0/legalcode).

THESE MATERIALS ARE PROVIDED "AS IS." The Trust Over IP Foundation, established as the Joint Development Foundation Projects, LLC, Trust Over IP Foundation Series ("ToIP"), and its members and contributors (each of ToIP, its members and contributors, a "ToIP Party") expressly disclaim any warranties (express, implied, or otherwise), including implied warranties of merchantability, non-infringement, fitness for a particular purpose, or title, related to the materials. The entire risk as to implementing or otherwise using the materials is assumed by the implementer and user.

IN NO EVENT WILL ANY ToIP PARTY BE LIABLE TO ANY OTHER PARTY FOR LOST PROFITS OR ANY FORM OF INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER FROM ANY CAUSES OF ACTION OF ANY KIND WITH RESPECT TO THESE MATERIALS, ANY DELIVERABLE OR THE ToIP GOVERNING AGREEMENT, WHETHER BASED ON BREACH OF CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, AND WHETHER OR NOT THE OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Introduction

This document provides a list of practical steps to mitigate human harms arising from digital identity ecosystems. It is a short companion guide based on the ToIP white paper *Overcoming Human Harm Challenges in Digital Identity Ecosystems* available here (https://github.com/trustoverip/hxwg/tree/main/harms) and at this permalink (https://trustoverip.org/wp-content/uploads/Overcoming-Human-Harm-Challenges-in-Digital-Identity-Ecosystems-V1.1-2023-05-04.pdf). As with the paper, all terms in **bold** are here in the glossary (https://trustoverip.github.io/hxwg/glossary.html).

1. Define the business case for harms reduction in your ecosystem

Human harms cost businesses and governments billions. Calculate the costs and benefits to your ecosystem and its stakeholders. Costs and benefits may include, but are not limited to:

- Costs: Customer care costs, regulatory fines and penalties, reputation management, insurance.
- Benefits: Reduced cost to acquire, increased customer, worker and community stakeholder loyalty and reduced churn, increased efficiency.

Set system KPI's to track these so that you can report on impact materiality in your ESG (Environmental, Social & Governance) accounting.

2. Ethics training for your team

All harms prevention stems from the team that are designing, developing, operating and commercialising the system. Give your team the skills and knowledge to think with an ethical mindset as well as a commercial one. Some quick resources:

- WEF – Ethics by Design (2020) - Contains many practical tools and techniques.
- Coursera – Ethics of Technology – Free training course.
- Markula Center for Applied Ethics at Santa Clara University - A Practical New Resource for Ethics in Tech Practice.
- Process Street, Minimum Virtuous Product checklist, (2021)
- Responsible Tech Resources ToIP Wiki
- Practical Ethics Expert Talk from Lisa Talia Moretti (2022) ToIP Wiki

3. Vulnerability Recognition

All harms affect vulnerable people more often and more severely than those who are more resilient, healthier or those who are not in crisis already.

- Have at least one shared objective for all ecosystem participants.
- Check that incentives for one group do not depend on harms to another.
- Carry out continuous risk assessments (see the ToIP Risk Assessment Worksheet (Excel format) and Companion Guide (PDF)), in particular for the most vulnerable ecosystem participants.
- Evaluate potential vulnerabilities by using an inclusion calculator and clearly identifying vulnerable groups (e.g. children, elderly).
- Monitor potential and emerging risks by offering a risk and harms reporting process that is open to all including those outside the ecosystem, this may be anonymous and/or supported by customer care processes and associated call reasoning codes.
- Make **guardianship** credentials available for use in the ecosystem. See Sovrin Foundation, Guardianship Credentials Technical Requirements V1 and Guardianship Credentials Implementation Guidelines (April 2021)

4. Edge agency

Many ecosystem participants are exposed to harm if they do not have freedom to autonomously and intentionally make their own decisions.

- Ensure that credential schema limit purpose for issuing and verifying.
- Include a non-digital or digital assist route to achieve the purpose or outcomes.
- Give holders time to make decisions, e.g. cooling off period, delay unlocking benefits.
- Revalidation cycles so that holders can consciously make decisions over time as things change.
- Include representatives from all participant groups in governance processes, e.g. democratic legislative processes.
- Enable participants to set their own limits (self-regulation) e.g. limit device usage/gameplay.

5. Balance of power

Any game where the rules apply unequally to players will result in harms to the weaker players.

- Deploy anti-coercion counter-measures e.g. verify the verifiers (e.g. using a **trust registry**), require non-repudiable evidence collection, require remote/proxy verification, and compliant holder agents. (See Anti-Coercion by Design, TNO 2020)
- Have an anonymous grievance, complaints or whistle-blower mechanism. Implement alternative dispute resolution (ADR) mechanisms with clear support for less powerful parties.

- Policies in the governance framework for the transparent election and selection of those who make the rules and enforce them.
- Jurisdictional balance of power, separate legislative, executive and judicial functions.
- Enable collectivization, ie enable individual participants to belong to groups and have representation within decision-making bodies in the ecosystem.
- Give participants access to experts and expert knowledge e.g. by employing participant advocates, offering training or independent advisory services.

6. Collective resiliency

Harms are infectious, therefore **digital identity ecosystems** must cooperate with adjacent ecosystems and have shared resiliency as a group.

- Predict: Carry out an ecosystem wide threat analysis and risk assessment
- Detect: Apply fraud management and fraud signaling techniques to harms e.g. have shared reporting metrics for abuse management systems with adjacent ecosystems
- Recover: Have an ecosystem-wide disaster recovery plan
- Prevent: Have common harms reduction principles and policies, report as a group on achieving harms reduction and impact materiality

7. Keep asking ‘What could possibly go wrong?’

Things will go wrong, harms will occur just as serendipitous and unintended benefits will arise, just by considering these harms as well as the benefits in your design you will reduce their potential to occur.

- In design use bad actor persona’s to test user journeys, or role playing and scenario building to consider consequences.
- In life you can track back from unintentional harms that have occurred by monitoring complaints from customer services, abuse management or worker grievance systems, and then using root cause analysis.

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.