

## Proposal for a session at the Future Internet Assembly

<b>Subject:</b> Scalable Trust for an open Future Internet
<b>Owner:</b> Zeta Dooly
<b>Scope (Max 5 lines text) :</b> Billions of global users, networks, services, data, and virtual entities have adopted the Internet as a primary mode of communication. A common theme of Trust emerged as a Grand Challenge in Bled in April 2008 across all domains: Future Networks, Service Infrastructures, Networked Media systems, Internet of Things, Experimental Test facilities. During Bled, it was agreed that Trust cannot be built in isolation or rely on technologies of one layer only. Trust must be maintained, monitored – whether created, obtained, assessed, measured or perceived – taking into account all information available. This highlights the need for convergence in cross domain challenges. Trust on the Internet reflects an end-to-end, context-dependent relationship between two or more entities enabled by intermediaries (networks, devices, services, applications). The proposed session aims to create a common understanding of what trust means, including technological, legal, business and social implications. It will bring together key experts from different fields and working at different layers to integrate their perspectives and debate their concerns. Principles of trust attribution schemes based on transparency and accountability and underlying issues like policy-aware trust architectures and assessment schemes, including identity management, will be discussed along with economics and usability balancing technologies to develop a trust framework that will support the Future Internet. For more details, see Appendix.
<b>Initiator domain:</b> Trust and security sub-group (Think-Trust)
<b>Priority from the originator domain:</b> High
<b>Duration of the parallel session:</b> 4 hours
<b>Other domains required to participate and how:</b> all domains – involvement in panel sessions
<b>Some possible endorsement/support from other domains:</b> Services sub-group

## Appendix I Scalable Trust for an Open Future Internet

Status of this document: for discussion in the context of Future Internet cross-issues

The Internet of the Future will be a conglomerate of heterogeneous current and future infrastructures (networks, services, data, virtual entities, etc) and of usages with mainly decentralized security and trust functions. The emergence of sensing and actuating devices, the proliferation of user-generated content and nascent (Internet-only) services delivery create the need to address trust and security functions adequately.

Trust on the Internet reflects an end-to-end, context-dependent relationship between two or more entities enabled by intermediates (networks, devices, services). This end-to-end relationship should be aligned to end-to-end scenarios throughout the development of the Future Internet so that trust dependencies are evident. It is within this sphere that it becomes obvious that a cross-domain approach to development of user scenarios will assist the development process, across services, networks, content and experimental facilities and each having trust and security challenges to consider. The layering (such as the ISO/OSI model) and late addition of security and trust functions have demonstrated their inefficiency in order to convey trust. Trust can not be built in isolation neither can it rely on technologies of one layer only. Trust must be created, obtained, assessed, measured or perceived taking into account all information available.

This calls for a more global rethinking and has become an evident priority for almost all ETPs (NESSI, eMOBILITY, NEM, ...).

Where does trust come from? In our societies, law and policy address complexity mostly through a combination of transparency, accountability and enforcement together with technological means in support of these. None of these mechanisms is perfect and unlawful behaviour is possible. However, violators can in principle be identified and held accountable. As a consequence, most of us follow the rules. Privacy is mainly based on laws and moral rules that give people the expectation that their data will not be abused and, if needed, legal redress is possible. Copyright protection includes, for example, fair use. In data mining, single data elements are in itself not secret or private, but combining information can be harmful. The essential point is that, in most cases, there is no a-priori mechanism that forces us to comply with legal or social rules. Rather we comply because rules are generally known and the social fabric tends to make compliance easier than violation. Globalisation and the existence of diverse jurisdictional domains diminish enforcement capabilities however.

Contrary to these mechanisms developed through history, current trends in the Internet lead to implementation of security and trust by ex-ante automatic access controls and technical reliance on secrecy. However, history teaches us to consider setting emphasis on usage rules rather than access rules or collection rules, and rely on the principle of transparency, accountability and enforcement in order to build trust in our Internet society.

Trust in the Internet relates therefore to several components, all of them of diverse nature depending on the agents or the jurisdictional domains: socio-economic values, network infrastructures, service infrastructures, content delivery infrastructures and governance. Interdependencies, levels of trust and levels of punishment for non-compliance are considerations that have emerged but weighting of priority or criteria for acceptance of trust boundaries are not clear.

At the basis of all these lie the principles of proper naming of entities (natural and legal persons, objects, virtual entities, devices, content, processes, applications, etc) and trust attribution schemes (identity management, authentication, authorization, accountability, reputation) .

In addition, transparency and accountability models (architectures, languages, policies) need to be developed in order to ensure technology functions as expected, to enable assessment of data (or content) usage at all times and to provide trust to the data owner or owners that legal redress can be successfully obtained in case of abuse. For this, basic capabilities need to be developed at the level of the network, software, services and their composition, and content management with the objective of allowing transparency of data usage and accountability. Underlying all this is the assumption that these models encompass sufficient flexibility to move pace with technical advancement.

Management of trust and security functions has to take into account the multiplicity of ownership domains (which traditionally defined the access and accountability policies) and of trust levels within these domains. There is a clear need for flexible and powerful models for service provision, data governance and system configuration allowing for affordable management functions. These functions have to be robust and scalable.

Trust in the Internet of the Future has a way forward in:

- interoperable (policy-aware) trust architectures from trusted communications to the application, including and beyond virtualization, to the data; These are the basic technology building blocks enabling trust.
- interoperable credential management infrastructures for entities (persons and objects)

This requires joint efforts from several domains:

- all: how to provide evidence of trust? By which means can we deliver trustworthiness: measurement, assurance, certification, proof, etc? On which set of languages do we express trust or security policies? How is this implemented across domains and across cultures? How to enable users to make informed decisions on the trustworthiness of the information? (make the concept of trust real, a physical entity, out of the virtual world).
- network: how to apply the end-to-end principle, allowing for carrying out the functions (accountability, transparency, logging, ...) at the most effective

locations in the network? How to map legal and social requirements from different jurisdictional domains onto policies?

- software and services: how to design systems that enable information accountability and appropriate use? how to make data usage transparent and accountable in dynamically composed services? Include end-to-end principal here as s/w and services will be key identifier of stakeholder scenarios. Need to integrate trust measures from different systems.
- content: how to extend the web architecture to support transparency and accountability and how to embed policies into content that allow for creativity, convenience, fair use and protection of copyright?
- test infrastructures: there is a clear need to test and monitor different policies and accountability mechanisms at a large scale.