



**Subject: Input received for "How to measure trust"**

*How to measure trust?*

*Contribution received from Volkmar Lotz – Trust & Identity*

**Title: *How to Measure Trust?***

**Problem Statement:** From the discussions at the previous FIA conferences, there can be no doubt that there is a broad consensus that trust in the Future Internet is essential. Without trust, FI opportunities will not materialise in new business platforms and models strengthening the European economy or novel applications increasing quality of life. The reason lies in the value of interactions over the FI for the stakeholders involved and its distributed ownership / federation, demanding entities to behave as expected in order to not put the values at risk.

A trusted FI, however, does not mean that nothing can go wrong: vulnerabilities of technical solutions are a fact of life (and there is no evidence that they will vanish with the advent of the FI), and they are likely to be exploited by malicious entities. The key to a trusted FI, thus, lies in the ability to assess the risk associated with these vulnerabilities and the likelihood of malicious behaviour as well as having means at hand to mitigate those risks by adequate controls. This allows a user, for instance, when consuming a service, to make informed decisions about the risk upon engaging in a transaction and to mitigate the risk if necessary (or withdraw from the interaction, if either the risk or the mitigation costs are too high).

If trust is considered to be the outcome of such a decision process, there is a need to capture the parameters influencing the decision:

- The value of an interaction – this requires to define what a particular interaction consists of and which assets are affected by it in which way. Interactions can be computations, accesses to resources, transactions, long-term relations, persistent storage, delegation of business processes, service calls and many other types
- The risk associated with the execution of the interaction – this expresses the likelihood and potential damage of misbehaviour of participating entities
- The available means for mitigating the risks, the necessary investments to deploy them (e.g., the cost of invoking a control service) and their impact on the likelihood and potential damage of misbehaviour

It is important to notice that this decision has to take into account the distributed nature of trust in the FI. Due to its lack of central control and the multitude of stakeholders in different roles, there are multiple anchors of trust, including applications, services, service delivery platforms, infrastructure, and devices.

The challenge for the measurement of trust lies in describing the nature of the related parameters (are they to be expressed in terms of values, properties, behaviours or others in order to allow informed decisions) and in actually capturing them in a given interaction context. When talking in terms of values, the challenge lies in finding sufficiently expressive metrics. A property based assessment of trust is likely to be sufficiently expressive and would allow to distinguish between guaranteed properties (capturing the notion of trustworthiness) and desired properties (required by a service consumer, say, from a consumed service for the consumer be willing to engage with the service, i.e., accept the remaining risk or trusting the service), but asks for capturing the deviation between two (sets of) properties.

The measurement of trust needs to be integrated in the architecture of the FI, spanning its layers and components. Thus, in addition to investigate into the nature of trust measurements, there is a need for defining and integrating methods, components and services that support the user in assessing trust in a given context:

- management methodologies and tools, ready to be used by the service consumer (services and users) and taking lifecycle and aggregation aspects into account (→ dynamic risk evaluation)
- a trust and security “toolbox” that can be flexibly adapted to the given business / risk context and allows to mitigate risks / increase trust
- methods and tools for assessing the effectiveness of a given selection and composition of controls
- their integration in FI architecture

We also need to investigate in the automation of the decision and mitigation process. The final decision is with the user, but it is infeasible to ask for user input each time, for instance, a service is consumed (these services are to a large extent consumed on lower layers of the technology stack). The establishment and management of user-friendly trust policies are required.

**Caretakers:** Markus Brunner, Michel Riguidel, Norbert Niebert, Pierre-Yves Danet, Theodore Zahariadis, Volkmar Lotz (author of this draft, alignment with other caretakers pending)

**Participants:** : same as listed in caretakers plus research community people invited to workshop in October 7 2009.

**Points of agreement:**

- Need to have less formal event(s) to explore greater synergies between research communities;
- Difficulties with parallel panel sessions during the FI Technical days (eg. T&I and Content or Networks);
- Between official FIA events, caretakers spend disproportionate amounts of their time dealing with administrative aspects eg. locating / inviting speakers and topics, instead of more pro-active and productive technical discussions amongst the members in the other FIA domains areas.

**Points of Discussion:**

Holding workshop on 7<sup>th</sup> October 2009 to prepare for FIA Stockholm with the following objectives:

1. To bring together FIA domain members (in a less formal setting than the FIA events) from the **Trust and Identity FIA community** with the members of the other FIA domains: **Future Content Networks, Management and Service-aware Networking Architectures, Future Internet Service offer, Real World Internet, Socio-Economics, Future Internet Research and Experimentation Software and Services,**
2. To provide an opportunity to review **cross domain Trust and Identity issues**, building on the achievements so far (in annex, list of documents from FIA Bled, Madrid, Prague, ..)
3. Allow for open and frank discussions on what the important **multi-disciplinary requirements and challenges** are for a Trustworthy Future Internet, especially in relation to privacy and identity, trust platforms and experimental facilities

**Follow up actions:**

**Reference:** In Madrid (Dec. 08) and Prague (May 2009), the Future Internet Assembly workshops held initial dedicated sessions on these topics, organised by the Trust and Identity caretakers.

Does this topic require a follow-up discussion in Valencia? Yes

If yes, specify draft title:

## **How to measure trust**

### **Input received from Syed Naqvi (RWI)**

#### **Problem statement**

*Insert here the problem statement: no problem = no need for a session! The length should be short, max 3 paragraphs of 5 lines. It should include and put in perspective 'the commonly' thought solutions to the problem or a reasoning behind the fact that there are no known solutions. History of the problem and background should not be included here, but in the reference section.*

As the topic name suggests "Measure Trust", we need to explore the probes/metrics that can be used to measure the trust value of the Future Internet-based infrastructures and applications.

Majority of current internet users hail from the non-IT community; the situation in the Future Internet arena will probably increase their proportion. It is therefore necessary to develop extremely user-friendly trust measuring tools that can be used by the general public. No matter how complex algorithms are running in the background, the output of these tools should be as simple as an automobile's speedometer or level of a battery's current charge.

#### **Points of agreement**

*List here the points of agreement and a brief explanation of why/how a consensus has been reached. Include as well significant options that have been left behind.*

Trust is considered as a social phenomenon and that's why there exists a considerable work related to the measurement of trust in the social context (Schechter 2007, Raimondo 2000, etc.). So we can deduce that there exists an understanding for having a mechanism to gauge trust. We need to extend the scope of this understanding to cover technical areas of the Future Internet arena.

#### **Points of discussion**

*List here the sub-points which are still under discussion as well as a brief explanation of the open options for each.*

Global idea for the discussion is to collect and harness recommendations of the experts working in the different areas of Trust such as computer scientists, network technologists, social scientists, legal experts, etc. The picture of TRSUT in the Future Internet arena is like a jigsaw puzzle whose pieces come from different actors working in the various aspects of trust. These disjoint pieces, if properly tiled, can give a clear vision of the trust in FI. We have to discuss the ways of envisaging the high-level picture of trust measurement methodology; a common approach/strategy towards its refinements; and clear understanding of concepts (including vocabulary & terminologies) among the various actors.

[Syed] Trust measurement often involves 'reputation systems'. We need to discuss the ways how 'reputation' can be expressed as a metric? How it can be normalized and eventually integrated into the overall Trust measurement probes?

#### **Follow up actions**

*List of agreed actions to do after Stockholm and before Valencia. These actions are to be undertaken by the 7 groups.*

There will be very limited time between Stockholm and Valencia meetings, so we have to make some rational expectations while defining the follow-up actions. It will be reasonable to expect that the team of contributors will show-up in Valencia with a draft skeleton of trust measurement methodology (with clear demarcation of probes and testing points) even in an informal format. But we need to agree on the timeline of this task in Stockholm.

## **Reference**

*References to external documents should be included here with a view to keep the overall text not longer than 2-4 pages. Include as well the presentations made during the conference.*

Schechter, L. (2007), "Traditional trust measurement and the risk confound: an experiment in rural Paraguay", *Journal of Economic Behavior and Organization*, Vol. 62 No.2, pp.272-292.

Raimondo, M.A. (2000), "The measurement of trust in marketing studies: a review of models and methodologies", 16th Annual IMP Conference, Bath (UK), 7-9 September.

Input received from FISE

### **8. How to measure trust?**

Trust is the basic ingredient of a successful transaction. Future Internet will enable transactions between heterogeneous networks and entities, belonging to different administrative domains. Hence, trust should be considered under a different perspective. Reliability will remain one of the key concepts of the future services. However, since the provision of many, if not all, services will require the composition of other sub-services as well as the participation of end-users, reliability will be hard to be assured and measured by a single entity. Trust among collaborating components/entities will play a key role in the estimation of a service's reliability and the allocation of responsibilities in case of failure.