



Coordination Action

Think Tank for Converging Technical and Non-Technical
Consumer Needs in ICT Trust, Security and Dependability

Plenary Workshop of Working Groups

FIAP, Paris, 09/10-SEP-2008
Hosted by TELECOM-ParisTech

Workshop Report, Issue 1.0

12-OCT-2008

Executive Summary

Think-Trust is a coordination action under the ICT-FP7 Theme. It deals with the achievement of user trust and confidence in the future Information Society and the Future Internet, through technical solutions that can contribute to the delivery of privacy, security and dependability. Think-Trust is supporting the RISEPTIS Advisory Board (*Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society*) mainly through the set up of two specific working groups contributing to the RISEPTIS objectives. WG1 is addressing "Security, Dependability and Trust in the Future Internet" and WG2 "Privacy and Trust in the Information Society".

The inaugural workshop of these two WGs took place in Paris on 9th and 10th September, 2008 and was attended by over 30 participants (including WG members, the [Think-Trust](#) project partners and the Commission). The main objectives of the workshop were to bring together representatives of the research community of security, dependability, trust, privacy and identity management (invited Working Group members) to identify and scope their future activities and discuss technology solutions in the path toward "Trustworthy ICT". Their work would also contribute to the RISEPTIS report; the activities of the [Future Internet Assembly](#); and, the [networking session](#) at ICT 2008 (25/27-NOV-2008, Lyon).

A number of important topics were identified at the workshop:

- Issues raised from WG1 included: the need for a *measurement infrastructure* at the network-, systems- and services-level for analysing and understanding the computational complexity of emerging threats and for using it to monitor the security status of a system and its services; technology solutions for addressing *the accountability* (responsibility) of service providers', users' and other stakeholders' activities but also of system behaviours/operations and of their applications; and, the creation of a *trust management infrastructure* together with adequate management policies and the *management and governance* of the Future Internet.
- WG2 identified an inventory of technology innovations which will be explored with regard to addressing the issues of privacy, identity management (IDM) and accountability in the information society. These included, amongst others, privacy transparency tool support, user-interface design according to privacy requirements, and a methodology for multi-party security/privacy IDM design. A path for further collaborative work has been identified and a subsequent workshop will work toward consolidating and progressing work in these areas.
- All the above require architectural support and possibly new legal frameworks for security monitoring, observability and measurability, as well as for accountability as they are not present in the current multi-layer, multi-domain architecture. The same applies for supporting dynamic trust management and user-centric privacy respecting interoperable IDM schemes.

Following on from the workshop the next steps are:

- submission of outputs to RISEPTIS, for consideration at their meeting in October '08;
- (*distributed*) WG meeting in response to RISEPTIS feedback, and to review WG agenda and development of discussions and position paper topics;
- presentation and discussion of WG orientations at ICT 2008, Lyon;
- collaboration with FIA sub groups on trust and identity matters;
- next workshop (early 2009, TBC).

Table of Contents

1	Context of workshop.....	4
1.1	Outline of project and its goals	4
1.2	Working Groups and goals.....	4
1.3	Workshop format and methodology	4
2	First Workshop: the objectives	5
3	First workshop: structure and discussions	5
4	Think-Trust WG preliminary perspectives	6
4.1	WG1 – Security, Dependability and Trust in the Future Internet.....	6
4.2	WG2 - Privacy and Trust in the Information Society	7
5	Overall conclusions and next steps	9

1 Context of workshop

1.1 Outline of project and its goals

Think-Trust is a Coordination Action under the seventh Framework Programme (FP7). It is concerned with the achievement of user trust and confidence in the future Information Society, and the Future Internet, through technical solutions that can contribute to privacy, security and dependability.

Think-Trust objectives include:

- to establish and to support an Advisory Board, *Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society* – RISEPTIS; the principal role of RISEPTIS is to generate a high-level report to EU policy makers concerning priorities for R&D and for possible legal and regulatory requirements; this report will be completed during summer 2009, in time for the new EU Parliament and Commission that autumn; further information on RISEPTIS can be found at <http://www.think-trust.eu/riseptis.html>
- to establish and support Working Groups of multi-disciplinary experts that will provide technical input to the generation of the RISEPTIS report.

1.2 Working Groups and goals

The goal of the Working Groups (WGs) is to contribute to the preparation of the high-level report described above, which is the ultimate objective of the Project and the RISEPTIS AB. Furthermore, these WGs will be serving as the main vehicles for further discussion of common cross-issues that were identified at the [Bled Conference](#), together with other research communities working in the field of the Future Internet.

WG1 – Security, Dependability and Trust in the Future Internet

WG1 covers conceptual and implementation aspects of multi-layered network and service infrastructures across the Future Internet design. These include technological evolution and scalability as well as the layering which will be required for polymorphic, physical, virtual and service networks. WG1 will also consider computing and communication paradigms, emerging threats, virtualisation concepts, and infrastructures and user-centric test-beds.

The prime focus of WG1 is technological, but there is also a need to take properly into consideration the underlying societal, legal, and economic issues and needs. There is an important synergy with WG2 in these concerns.

WG2 – Privacy and Trust in the Information Society

WG2 covers privacy and trust, global persona management and identity management. These will be examined both from the technical perspective and from the user perspective (user centricity). WG2 will cover concepts, implementation and tradeoffs within human/machine/device ID (+ multiple persona) management; data collection, data storage, data access and data protection rights for businesses and consumers; Usage facets: authentication, privacy, confidentiality; personal privacy versus societal and national needs; and standards and regulatory issues.

While principally considering the technical aspects required for the user, this WG will also consider the “non-technical” needs and concerns, from social and economic viewpoints (costs vs. benefits quantification), from the human and personal to the organisational and legal/governmental perspectives across varied application domains and enabling technologies., for example, biometrics, crypto, data/identity rights management, trusted computing and communication.

1.3 Workshop format and methodology

The working groups were established through a competence assessment process that began in April 2008 with a consultation process between Think-Trust, the Commission and RISEPTIS members. Two months prior to the workshop, each WG held an audio-conference meeting to kick-off the WG and agree on the workshop approach. A request was given to all Working Group members to submit a position paper and a presentation to the organisers of the workshop. This request was extended also to those members who could not be present in Paris. The members were also requested to provide additional feedback on their areas of expertise, research interests and topics considered of major importance to a European Information Society, and to the Future

Internet, particularly in a European setting. Including the project's position paper, which was provided ahead of time as a thoughts stimulator, twenty six position papers were received, and published to the WG members (see Annex C).

It is worth noting that a natural overlap exists between the trust considerations for WG1 and the privacy concerns of WG2; in particular, when the *management* of trust and identity is deemed to also incorporate the *construction* of trust and identity. This overlap is limited as there is a common theme of trust, however, within different scenarios and it must be remembered that there is a sizeable gap between the WGs in many regards.

2 First Workshop: the objectives

The inaugural workshop of these two WGs took place at FIAP, Paris, on September 9th and 10th. It was hosted by TELECOM-ParisTech and was attended by over 30 participants (including WG members, the [Think-Trust](#) project partners and the Commission). The list of workshop participants may be found in Annex B.

The objectives of the workshop were:

- to provide a first face-to-face meeting of the Working Group members, and initial community building activities;
- to generate initial input to the RISEPTIS report;
- to generate inputs, contributions, discussion and consensus towards ongoing Working Group activities, for example, the agenda for the WGs; work items; and actions.
- to generate inputs and contributions to European Commission activities and events:
 - future Work Programme (post-2010);
 - the Future Internet Assembly – see <http://www.future-internet.eu/home.html>;
 - the Think-Trust [Networking session](#) at ICT 2008 in Lyon.

3 First workshop: structure and discussions

The agenda of the workshop is found in Annex A.

Following overviews of the Think-Trust project by Zeta Dooly, the project Coordinator, and of its context by Thomas Skordas, from the Commission, the WG1 leader, Prof. Michel Riguidel, and WG2 leader, Prof. Neeraj Suri, summarised the positioning of the WGs and set the respective objectives for the workshop.

The authors of the position papers gave short presentations (see Annex D) to the combined meeting in two consecutive (WG) batches, each followed by a discussion session. A number of position papers whose authors were unable to participate were briefly summarised by the WG leaders so as to include them in the initial discussions. Based on the discussions, the outline structure for the second day was agreed to include parallel sessions of the WGs to arrive at their sets of findings before coming back to a plenary session to summarise and to conclude the way forward.

Preliminary advice was given to this workshop to concentrate on technical matters, and to avoid speculation about legal and regulatory issues and requirements. The technical considerations may indeed subsequently give rise to regulatory needs, but that should not be a constraint or pointer at this stage.

Three common assumptions were agreed when considering the Future Internet:

- it will be a pervasive, digital environment, composed of multiple heterogeneous infrastructures and technologies;
- we cannot anticipate what entities, protocols or business scenarios will be entailed in the Future Internet;
- user-centricity is a critical consideration and goal.

The initial focus of the discussions within the WG parallel sessions were presented by the WG leaders and centred on the following areas:

WG1

- Measurability, Metrics, Transparency
- Accountability/ Responsibility
- Trust Management & Governance

WG2

- Identity: Provision & Management
- Privacy & Security
- Info/Data Accountability & Governance

A full discussion of these perspectives was the focus of the plenary session on the second day.

4 Think-Trust WG preliminary perspectives

Following the individual presentation from participants of their own research position papers and then an initial group session, there were parallel Work Group sessions in which themes were prioritised for moving forward. The outcomes of these discussions are summarised below.

4.1 WG1 – Security, Dependability and Trust in the Future Internet

WG 1 members came to a consensus on building on the sub-headings presented by the WG leader in the initial session. The main topics addressed in the presentation covered the areas of Future Internet design, which will be heterogeneous, pervasive, open, and trustworthy. This results in the research challenge of developing new architecture based on societal needs, user experience and value protection. The WG prioritised future research challenges for further work. These include:

4.1.1 Measurability, Metrics, Transparency

While up-to-date statistics would be useful as a starting point for the measurement of any secure/insecure entity, these are in fact scarce and available test data are often out of date and misleading, not being based on recent real-life measurements. Reasons for this lack of data include: rapidly changing attack modes; victims of attack typically not disclosing information, as well as inherent privacy issues contained therein proprietary data whose sharing and exposure may affect company competitiveness; and, the sheer complexity of distributed attacks.

Work on measurement of TSD-related factors is needed in order to get a better understanding of priorities for technology R&D plus actual deployment. Work already under way in this area needs to be reviewed, and possible approaches examined that could address metrics and what is to be measured, scope for a measurement and monitoring infrastructure, analysis of attack and failure, the economics (costs and benefits), and tools for incorporation into network systems and services that will contribute to their transparent behaviour.

A corollary of monitoring the Future Internet is that privacy concerns are inevitably raised, with a balance between accountability and opacity being required. Any measurement of security, therefore, must be implemented by a well designed mechanism to find this equilibrium. A further constraint is the need for comparative security metrics, which implies that quantitative, as well as qualitative measurements are needed.

A generally applicable approach to increased transparency (and hence trust) developed, concerning the provision of facilities for the accessor to verify certain 'claims' made by the accessed entity, with respect to, say, its handling of personal information.

4.1.2 Accountability and Responsibility

Accountability is fundamental to developing trust in ICT networks and services. All actions and transactions should be ultimately attributable to some user or agent. Accountability brings greater responsibility to the users and the authorities, while at the same time holding services responsible for their functionality and behaviour. It is noted that in addition to necessary technical mechanisms, there is a requirement for legal and regulatory backing to provide for appropriate sanctions and redress.

Accountability mechanisms naturally encounter problems if large amounts of data are being logged. There are also inherent privacy concerns surrounding the disclosure of such logs. When establishing a means of redress via these accountability/responsibility logs, a business-level model might therefore be adopted. Lessons could be learned from the insurance sector, where any action

taken must be observable by all parties involved, and where visible rules and policy awareness are a prerequisite.

Such observable action and familiarity with regulations will not be made any easier in the 'Internet of Things', where various heterogeneous devices will be present. Thus, there is a strong requirement for architectural support if accountability and observation are to be delivered in the Future Internet. Such provision is lacking in the current multi-layer, multi-domain architectures.

Interoperability between accountability domains will possibly require new work in technical standards together with possible regulatory support.

4.1.3 Trust Management & Governance

Primarily, a workable definition for trust is required; which may be linked to accountability and governance but also to the dependability of systems and their operational transparency. Common languages / translators and protocols for trust policy, specification and negotiation would be a good starting point. This would then allow the construction of trust as an entity itself.

Localised (contextualised) individual points of trust can be used as collective indicators and, for example, be leveraged to measure the consistency of multiple (potentially trustworthy) actors. Multiple channels could also be used, in line with the concept of 'out of band' signalling.

A number of temporal aspects of trust must also be managed, given that any degree of trust accepted may only be on a short term basis, especially in real-time scenarios, as well as the fact that it may be only determined using incomplete/delayed contextual information. The trust lifecycle, incorporating the formation and breakdown of this trust, must therefore be fully supported, with dynamic contextualised, distributable and understandable policies in place to implement dynamic contextualised trust.

4.1.4 Architectural issues

Architectural support must be provided for trust and privacy aspects of the Future Internet: first, with regard to transparency - security monitoring, observability and measurability and for data logging and log access; second, with regard to the ability to function across multiple layers and domains, as well as having policy awareness and transparency as architectural properties.

Architectural support for dynamic, contextualised trust is needed; this entails requirements for tools and standards to express and to deploy interoperable policies, together with the tools necessary for distributed trust interrogation and verification.

The requirements for accountability illustrate these needs: though the user can be fully accountable within the defined local context, the privacy of the user must be protected by that local domain, and inappropriate or unauthorised logging and tracking information should not be made visible outside. Where there is a need for external accountability, for use of a remote service, say, then the specifics should be set as part of the service agreement for service access in line with (possibly dynamic) policy agreements between the domains.

4.2 WG2 - Privacy and Trust in the Information Society

The approach adopted by WG2 was to review the items presented by the WG leader on Day 1 and it was agreed with the WG members that solutions to these 3 areas;

- Identity: Provision & Management;
- Privacy & Security;
- Info/Data Accountability & Governance.

These were interdependent, and could not be discussed in isolation from each other and thus seven primary topics/solution areas were identified. It was agreed that the scope of WG2 for the initial period would need to prioritise these further (a weighting/voting process facilitated this) in order to focus the work.

The members agreed the next step would then be the expansion of these topics by identifying a champion for each of these sub-set areas and working toward progressing outputs from this initial WG session. It was also decided that WG2 will work very closely with WG1 in areas of commonality and synergy between the two WGs.

The following topics were selected by the WG2 members for initial work areas (in weighted order):

4.2.1 Privacy transparency tool support

Tools for supporting privacy transparency are required for individuals and Data Protection Officers; these include tools for enforcement and dynamic consent management. The right for individuals to access their personal data from data controllers is a cornerstone of the EU Data Protection legal framework, but in reality there has been little consideration at the system design phase about how these rights can be effectively, safely, and conveniently exercised by data subjects.

The reality is that many people today do not know who has access to their personal information. Even if users can see their data, they may have no control over it; i.e. to remove / delete / amend what they deem inappropriate or false. A privacy transparency tool must incorporate dynamic consent management and be built into the architecture of any identity management system.

User-centric identity management, providing strong mutual authentication between data subjects and data controllers is a pre-requisite, however more research is needed into how personal data should be stored and structured by data controllers to maximise the transparency available to individuals, and to minimize the costs and burdens of fulfilling access requests. Increasing the depth and scope of the personal data available to data subjects online may increase privacy risks unless accompanied by a holistic approach to system security design. However there is virtually no literature directly addressing these topics.

4.2.2 UI design according to privacy requirements

There is currently a lack of research in user-interface design based on users' privacy requirements. Meaningful and understandable controls are required. Strong authentication, without the need for strong identification is one goal (i.e. non-declarative, strong authorisation). There also exists a need for tools to assess risk. For example, how do we know what is happening in a data controller? Could a PKI be implemented for a data controller?

It was noted that current policy statements from service providers are not designed to be understandable by the users, but to get access to their desired service or information; users accept, with a tick-in-the-box, privacy policies that may well not be in line with their needs.

Interoperability and consistency of privacy policies calls for tools and standards as in (4.1.4), above

4.2.3 Methodology for multi-party security and privacy IDM design, including metasystem standardisation

This topic area is concerned with how to design comprehensive and coherent privacy-protecting identity management systems correctly, from scratch, assuming one does not have to cope with legacy systems.

The multi-party aspect concerns the fact that any transaction typically involves multiple parties (eg, clients, servers, peers, notaries, etc.) based in different security domains under different privacy regimes, each involving different identity providers and policy rules. The topic area includes the meta-system issues raised by the need to interpret, translate, and optimally reconcile policy rules, statements, and terms expressed in different languages to represent different semantics across the different domains of the parties involved. Resolving such issues will clearly require common cross-domain standards.

4.2.4 "Minimum disclosure" credential management

Although theoretical approaches and some prototyping do exist, we are still far from deployment in practice through lack of common UI design and policy standards (See points 4.2.2 and 4.2.3, above).

Basic cryptographic designs exist to build credentials that can be used to support user-centric, limited disclosure of identity information. These need to be complemented by suitable open standards and semantics that can be leveraged to create an ecosystem and a market that will justify the investment for developing necessary products.

A consequence is also that if minimum disclosure is 'per situation', then authentication requirements are also specific (and minimised) to the needs (and context) of what is being accessed.

4.2.5 Virtual social control, e.g., virtual neighbourhoods, including reputation systems

If the future internet were to become a multi-tier system consisting of a highly controlled and mostly automated part and a creative but inherently insecure part, research must be done to understand how social disapproval and negotiation mechanisms can be implemented in the future *creative* internet. The practical aspects of research include virtual social interaction environments, reputation generation and maintenance, negotiation, forgiveness, and restitution. The main aim is to facilitate trust and understanding.

4.2.6 Non-declarative strong authentication

There is a clear need to replace username/password login by stronger schemes while not exploding the costs for authentication supported by services providers. Today, users can select any credentials they like in a "declarative" way. This brings an advantage to allow anonymous usage of services, but it also comes with major issues and crime risks for large services like Web mail or web-based applications. "Non declarative" authentication mechanisms can be biometrics, two-factor authentication (what I know + what I have) or new schemes to simplify login. The goal is to ensure that traceability, when required by policies, will be possible. The internet is not a special case in our society. Protecting privacy does not mean zero-accountability. Policies will define where traceability is required and a strong authentication mechanism, responsible and non-repudiable, is highly needed.

4.2.7 Privacy friendly biometrics– "One way" enrolment & usage protocols

While a biometric process may not completely eliminate duplicate enrolments, they are, nonetheless, a continuous means for identification. 'Supervised' enrolment protocols may well be incorporated into identification and authentication systems, based on biometric processes. Carrying out cryptography separately from biometrics has the virtue that one is decomposing the solution into two simpler, well-established problem domains. However, owing to the inherently noisy nature of biometric templates, doing crypto and biometrics separately would appear to require using a central database of biometric templates if the design goal is unique enrolment of individuals, in order that matching can be done against previous enrolments. In summary, this refers to a system where you could capture a live biometric on someone, together with a hardware token, and without a central template database. It would be a breakthrough to have a practical design where it was not logically necessary to have database of templates in order to implement unique (i.e. non-duplicated) enrolment of individuals (in some application domain). When discussing privacy-friendly biometrics as a possible solution area, it was agreed that a clear distinction must be made between supervised biometrics (e.g. border-control) and unsupervised biometrics/registration (e.g. building-access using retina identification). The trust relationship between the stakeholder./user and the registration source (e.g., government, bank, organisation) is a key consideration factor here.

5 Overall conclusions and next steps

Feedback from participants was collected at the workshop as to the usefulness of the discussions. The WG participants expressed significant interest in taking this work further. Champions have been appointed in some of the areas identified. If you would like to volunteer to champion any of the areas in this report, please contact the WG communications leads: WG1 khowker@tssg.org; WG2 jclarke@tssg.org.

An update of this workshop report should be in a position to include additional input from these champions. The following agenda for further continuing the work of these WGs has been established to a degree, although this is somewhat flexible as the environment changes. Further activities and contributions are expected from WG members in the near future in the following areas:

- input to RISEPTIS next meeting and report;
- development of discussions and position paper topics;
- development of representative cases/story-boards; these apply back to explore the topics and themes and their relationships;
- provide input to the [Think-Trust Networking session](#) at ICT 2008 in Lyon, which will be an opportunity to inform the participants of the progress made in the WGs and obtain feedback from the wider community;
- collaboration with FIA sub groups on trust and identity matters. For example, [Services and Architectures WG](#).

Please make a note of the upcoming events – for more information, see [website](#)

- meeting of RISEPTIS advisory board, 23-OCT-2008, Athens (RISEPTIS Members only);
- WG meetings (phone conference) in response to RISEPTIS feedback, and to review WG agenda and development of discussions and position paper topics (WG members only);
- ICT 2008, 25/27-NOV-2008, Lyon;
- Networking Sessions – liaison and dissemination 26-27-NOV-2008 (exact date/time of Think-Trust session - No.184 - still TBD);
- FIA Madrid 09/10-DEC-2008;
- Next WG workshop (in first quarter of 2009);
- [Future Internet Conference](#), 11/13-MAY-2009, Prague (NOTE: scientific papers due 30 October 2008 – see call for papers)