

*Grant agreement number: 216890*



*Project title*

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

*Instrument*

Coordination & Support Action

*Deliverable reference number and title*

D2.4 Plenary Workshop\_2\_WG

*Start date of project: 1<sup>st</sup> January 2008*

*Duration: 30 months*

*Organisation name of lead contractor for this deliverable*

Waterford Institute of Technology

## Executive Summary

The second workshop of the Think-Trust project Working Groups (see [Annex 1](#)) took place in Brussels 24/25-FEB-2009, with over thirty invited participants.

The main goal was to provide findings and recommendations for input to the RISPEPTIS advisory board for its report, and to feed into the thinking and planning of future research in the Framework Programme. The approach was to work on four *use cases*, proposed by [RISEPTIS](#), together with material from related sources – current projects, the FIA initiative, and ICT2008, etc.

The use cases cover the trust and security needs for electronic identities, the challenges of joined-up health services, Cloud computing, and the nomadic and mobile user. All make the European user and citizen central to their concerns, but each also looks beyond, to the global context.

The two Working Groups concentrated on two use cases each. The result was four sets of findings, mainly research challenges, covering the medium and longer term needs.

Taking as given the general statement of the needs for trust and security, a number of fundamental areas were identified. The conclusions were summarised in two groups: the first mainly from the user standpoint, with the second looking at means of supporting the users' needs. This outcome corresponds well with the scope of the two Working Groups.

The headline concerns in the first group are typified by eHealth where the user/patient is right at the centre of considerations, with certain rights, duties, responsibilities, and controls, together with the generic problems of provision, use, and management of all aspects of identity – from human users to inanimate entities. These resolve mainly into matters of privacy and data protection, with rebalancing the transparency of users and services, and also the need for support of the user in an increasingly complex and difficult environment. The wider needs of privacy concern the protection of all aspects of identity-related information, not only the prevention of unauthorised or unintended disclosure of the primary parameters of identity, but also limitations on building quite unique identifying or identifiable profiles by amassing and aggregating snippets of information trails that users currently leave behind. Similarly, data protection is not only about technical prevention of disclosure of personal information, but also about the responsibilities of those responsible for handling, processing or storing it.

The second group centre on what is needed to support the nomadic, mobile user, and to enable the trusted use of Cloud-based services. A number of key characteristics and requirements are identified, together with an indication of possible regulatory support. These highlighted the need for an architectural framework for trust and security, with the use of virtualisation to maintain separation between entities in an environment where physical boundaries have broken down. Continued development of underlying technologies is needed to keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment. Accountability, that should be respectful of privacy, is seen as vital in ensuring transparency, deterring malicious action, and providing diagnosis of failure. A specific need for automated security policy governance was identified, extending from the formulation and agreement of what is to be provided with respect to aspects of trust, privacy and security, through the monitoring and reporting conformance of operations, and on to remedial actions for non-compliance.

## 1 When and where?

**Location:** BU25, Avenue de Beaulieu, Brussels.

**Start:** 24-FEB-2009; 09:00, **End:** 25-FEB-2009; 12:30.

## 2 Participants

See [Annex 2](#) for the full list of participants.

## 3 Target results of workshop

- Overall: Contributions to the RISEPTIS report in the areas identified in the actions arising from the Athens meeting
- Take account of material from related initiatives and sources:
  - the RISEPTIS use cases;
  - related projects;
  - FIA;
  - ICT2008.
- Deduce guiding principles and challenges from the use case material
- Development of material:
  - analysis, and identify/fill gaps;
  - derivation of requirements, issues, etc.;
  - consolidation of commonalities and conflicts;
  - feed-back to and development of sources.
- Identify a first set of priorities for 2015+ research.
- Forward plan for WGs

## 4 Agenda

See [Annex 3](#) for the workshop agenda.

## 5 Workshop proceedings

Following a brief introduction and recapping of the *Terms of Reference* of the Working Groups, the conclusions of the first workshop, held in September, 2008, were presented.

A presentation was also made by Ms. María Verónica Pérez Asinari, Legal Adviser to the EDPS (European Data Protection Supervisor), which gave a useful and relevant<sup>1</sup> overview and update on current European positions on data protection entitled: "[Some key issues to keep in mind and their interaction with \(new\) IT challenges](#)". This presentation covered a range of topics including: what constitutes personal data; applicable law; the actors - data *controller*, -data *processor*, data *subject*; what is data protection? – obligations, rights, exemptions and restrictions, remedies.

Discussions then commenced on the four use cases. In order to stimulate the discussion, each use case champion made a brief presentation outlining the main points in their use case area. Background information, likely future trends in the area and a roadmap on how to achieve such visions for each use case were also distributed to the workshop participants in advance.

Two use cases were allocated to each WG, with an outline of each particular area, written by the assigned use case champion.

WG1:

- **Cloud Computing** (*champion*: Sachar Paulus)
- **Nomadic working and living** (*champion*: Michel Riguidel)

WG2:

- **e-health** (*champion*: Xavier Larduinat)
- **ID Management for e-Government** (*champion*: Kai Rannenberg)

The chief goal of this second workshop was to gain an insight into the requirements, challenges, issues, barriers, priorities, etc. for each use case discussed. These insights would be of a technical nature, but would also capture the personal, social, economic and policy/governance issues arising in each, all the while placing an emphasis on the end-user/citizen.

The use cases would be examined in their own right, as well as in the context of being inputs to the RISEPTIS report.

WG perspectives on the use cases – a suggested sequence of sessions was given:-

- initial analysis/orientation
- develop future scenarios
- derive technological challenges, issues, R&D priorities, etc.

Groups should concentrate on their specific *Terms of Reference*, identifying the issues and priorities for *up to and beyond 2015*

A short plenary would align the two groups and set out the plan for the second day.

The final Group session of the second day consolidated the work from the previous day. Groups were asked to identify, for each use case, shorter and longer term research priorities and cross-research issues between the use cases.

The final plenary session would consider the presentations from the two groups, and seek to consolidate findings; identify common issues; and integrate R&D priority recommendations.

---

1 *Useful and relevant*, in that the material was referred to frequently during the Group sessions, and Verónica herself was able to take an active part in the Group discussions during the first day.

## 6 Summary of Group Sessions

### 6.1 Working Group 1 – Security and Dependability in the Future Internet

#### 6.1.1 Cloud computing

Initial points concerned a refinement of the definition of Cloud computing, as well as the identification of gaps in and possible issues relating to:

- the concept of software-as-a-service;
- the need for operator agnosticism and interoperability; and,
- the role of virtualization.

#### *Discussion points*

- Cloud computing is, to some extent, an invisible population of services – both functional and storage. Without some formality, it will be a chaotic wild-west environment.
- Structure and governance is required such that a workable, responsible framework can be established. For example, every month a company may automatically seek out the (multi-factorial) ‘best’ service to run its pay-roll. For this, very high standards of trust are required, including appropriate assurances of legal compliance (and/or indemnification). The requirement is *business trust v. transparency* – the capability to balance *benefit* against *risk*.
- Sub-Clouds (domains) within the Cloud are feasible.
- How is the ‘Chinese wall’ concept, familiar in the finance sector, to be realised in the Cloud?
- The RESERVOIR project [white paper](#)<sup>2</sup> was noted as an overview of a Service Oriented Infrastructure.
- Compliance requirements include:
  - Expression and agreement/acceptance of policy. For example, by SLA;
  - Automation of process and action; notification of fault/failure; and,
  - Mechanisms for remedy. (The insurance industry may have a role here.)
- There is a requirement for personal privacy, *simultaneously* with law enforcement and national/regional security needs. This is not a simple zero-sum game – certainly not until technological possibilities have been fully researched (or rather, exhausted).
- To make the anticipated personal profiling at least more difficult, garbage collection facilities should gather the digital detritus that we may unknowingly leave lying around.
- Although the technological paths are not yet established – how-to? and what? – *measurement* is seen as a vital building block for trust establishment and maintenance.
- Business model considerations should be separate from technological possibilities.
- Legal context and considerations:
  - WTO framework (merchandisable);
  - Data controller has the rights and liabilities for sub-contractors;
  - User has to go through entity who provides the Cloud services and act as a data controller;

---

<sup>2</sup> Accessing this document requires user login

- Legal compliancy: transparency;
- Mapping legal policy to technical policy;
- [Consequence project](#) (with Microsoft as partners);
- Machine-controllable policy (Is it acceptable?);
- Person-controlled policy deployment is not scalable.

### 6.1.2 Nomadic Working and Living

This use case can be seen as complementary to the Cloud: nomadic front-end + Cloudy back-end. It should be examined from the perspective of a generic user and his communication/access device, as well as the resulting trust issues.

Nomad-ism (Nomadicity) is with us now: a mobile phone is already a multi-media device offering access to many services and providing its own local facilities – identity and location, personal data, cash and payments, etc. There is, therefore, already a wide range of security and trust challenges and issues. Vulnerabilities include device-dependency, loss and theft, virus attacks and service unavailability. There are a number of facets to the complexity of integrating and managing security in this field: real time, *in vivo*, just in time; usability – how to deliver usable (dynamic), contextual security and trust in a personal device; regulatory issues – jurisdictions, domains, policies.

#### *Discussion points*

- Privacy of mobile/nomadic users:
  - Security of end devices: proliferation of intelligent devices; 3G terminals, PocketPC, PC, etc.; personal trusted entities (next generation smart cards, etc.); wearable and/or transportable embedded systems, mobile robots, etc.;
  - Security of end-users: Identity & Authentication of ontologies & sociologies; virtual identities (TPM for hw, Smart card for persons); biometry at large;
  - Privacy and traceability;
  - Unobservability and unlinkability;
  - Usability with diversity (diversity in Europe);
  - Ethical issues: illicit content, illicit computations, legal proof, content control & filtering; security in obscurity - we must not be hostages of one security mono-culture; security sensors manageable by end-users to “measure security assurance”;
  - Digital Sovereignty: auditing; proof of the past, authentic memory of an information system, auditability of a database; access control & filtering, security of content (IPR, DRM, etc); filtering of viruses, unsolicited contacts & messages (spxx : spam, spit, spim, etc).
- Current situation:
  - Security facilities in: mobile telecom operators, WiFi, Internet – TLS/SSL YTPM, smart cards, secure OSs;
  - However, security is under-utilised (no business case?); there is a lack of standards; current systems are not scalable or pervasive; they lack ID management and multiparty security; there are no controls of traceability; they are dependent on mobile devices (phone); they is disproportionate responsibility and transparency balanced against the user.
- Future needs and solutions:
  - Monitoring and control of traceability/linkability;

- Accountability – fully interoperable, implying controls and privacy-sensitivity at architectural levels
- Context-aware trust/security provision designed in, with usability tools and automated policy implementation (how to respond to changes and how inform the user);
- Everywhere/everyware security and trust that is pervasive and ubiquitous: anywhere/anytime/anyhow – do it here, store it there, multi-model and platform agnostic.

## 6.2 Working Group 2 – Privacy and Trust in the Information Society

### 6.2.1 e-Health

Discussions were based on a real-life example of an e-Health-Card system established in Slovenia that had already resulted in tangible benefits for all stakeholders, but that will be further developed to take advantage of new technologies and policies. The building and operation of a chain-of-trust between the patient and all practitioners and clinical and administrative services was seen as the central concern.

#### *Discussion points*

- Chain of Trust mechanism: refers to trust in the entire ecosystem, (not just A trusts B, B trusts C, etc.). There is a need to focus on real elements within the trust environment: data storage at any given time; securing patient health records – is it just PKI or is more needed? How is this to be managed?
- Data retention issues: who manages/constrains the future use of data? Is data access to be transaction-based *and deleted right after use*? Implications of the EU's [Article 29: Data Protection](#) need to be cross-checked.
- Trust needs to be built in from the start, and extend across all modules of the design and building on early real use cases. Collaborative health-care will involve a wider set of actors than the patient and practitioner, with the possibility of active virtual entities.
- Fundamental technology requirements for: ID management; responsibilities for patient data; secure data handling; trail of accountability for all stages of 'transaction'; response to patient status/context.
- Control of access is a key requirement: authorisation control and definition of strategies, including default consents in emergencies, is needed; definition of roles and responsibilities of all stakeholders?
- 2015 Vision:
  - Defined access control strategies; design of access strategy management: defined parameters for all actors; data storage facility to define access strategy; privacy rights and responsibilities for every stakeholder; user involvement in control of access.
  - Privacy-friendly crypto: attribute management to avoid unintended identification; mutual authentication techniques to support proper dialogues between all parties; simplified credential definition and usage to allow a range of privacy control through policies and automated tools – from full disclosure to anonymity via à la carte.
  - Supervisory bodies with authority to manage and adjudge conflict and complaint, particularly with respect to privacy abuse. Sociological issues concerning attitudes to technical solutions; for example, distributed (possibly Cloudy) patient health records. Delegation controls, ultimately with the patient in charge, including accountability.

## 6.2.2 Identity Management for eGovernment

An overview was presented that set out a roadmap from the current position with government ID (paper) documents and electronic IDs, via extending e-ID credentials to objects and legal entities, thereby leading to an integration of e-ID credentials with government ID 'documents'.

Accompanying measures include: adding user-centric privacy-enhancing technology to government IDs; the need for an identification meta-system; and, developing policy support for relying parties.

### Discussion points

- How to bring together government-provided entities and those from private sector? Should/could **.gov**-issued credentials be used in **.com** tokens?
- Building on an eGov approach is essentially top-down. A complementary, flexible bottom-up would allow for combining secure (trusted) **.gov** credentials into a user-centric scheme.
- Peer-to-peer e-ID authorisation (authentication) using NFC technologies that leave no trace is currently feasible: does this indicate a general principle?
- Multi-purpose, multi-authority certificates may be built from government-issues cards.
- Multi-domain/authority (E.G. cross-border) ID management considerations: credentials could be attached to existing tokens; who is then responsible? Is the smart card the best vehicle? Government initiatives – on line search and return to localised platform, de-materialise border control?

## 7 Final plenary session – Summaries and Priorities

The Groups had been asked to summarise and prioritise the main issues from their use case discussions:-

### 7.1 Cloud computing

#### 7.1.1 Significant areas

1. Automated policy governance
2. Privacy-aware accountability infrastructure
3. Measurability & assessment

#### 7.1.2 Issues

- The legal context is undefined and together with high complexity, this leads to a necessity for:
  - Standardized clauses;
  - Automated processing;
  - SLA automation with integrated security and privacy;
  - Compliance requirements being mapped to technical policy (controls); and,
  - Data centric policy enforcement.
- The increasing volatility of relationships means “bad-guy-tolerant” and assertion vs. identity infrastructures are needed, as well as context-based access control (*proof of ability/permission*);
- *Share and you will get more* thinking implies cheap/inadequate Cloud security. Investigate business incentives: how far we can go functionalizing security (services vs. infrastructure);

- Explosion of identities and devices means support for identity aggregation on devices (multiple personae issue), as well as location and sensors. Both offer opportunities and risks by providing environment transparency/disclosure.

### 7.1.3 Research opportunities

#### 1) Architecture:

- a) Common, open architecture, including free code, specifications, construction and verification methods, as well as tools for the Cloud. Test scenario: Migrate Cloud enterprise applications in real time.
- b) Attaching policy information to data. This would require research into the interoperability of data formats and platform independence.
- c) Dynamic federation between arbitrary technologies and sources of trust; towards one-time-credentials and assertion mechanisms, without disclosing personal / identity information.

#### 2) Methodological:

- a) Improve and spread technologies to both fulfil multiparty security requirements such as (public) security **AND** privacy.
- b) Measure and/or assess security and privacy - standardized methodologies.
- c) Develop and spread methodology to plumb in security (and other non-functional requirements) for Future Internet projects.

### 7.1.4 Visionary Approaches

Where: 1. *Computing / storage / data access is not an issue*

2. *Sufficient information to provide a direct link between digital and real world*

- Use *automated reasoning* to digest security information (raise detection vs. prevention).
- Consider the stability/dependability of the whole *system* (perhaps via *inherent diversity*).
- Data mining & aggregation, deep crawling; giving rise to a need for transparency for societal values at risk (autonomy, privacy, etc.).
- Security by compartmentalization.
- Data warehousing, deep crawling & semantic web; means a need to review accountability in that context

## 7.2 Nomadic Working and Living

### 7.2.1 Goal 1: *hic et nunc* (here & now) security – privacy and trust issues

To protect our volatile digital life and environment, *in vivo*, in real time, the following issues must be considered:

#### Short-Term

- Trusted secure tokens & device (sensitive device): multiparty; massive collaborations.
- Location as an alibi: Location is a privacy issue, traces of trajectories, observation of behaviors (maps, satellite images, city cameras)
- Usability: explicitly-aware security; e-Inclusion (3.6 billion GSM users: on/off?)

*Medium-Term*

- Dependency, addiction and bias due to the digital world; just-in-time security, “crisis” management
- Privacy of personal, sensitive communicating devices: Internet of Things; delegation of security to nomadic personal robots; swarms of objects; body area networks (medicine).

⇒ **Trust Infrastructure**

**7.2.2 Goal 2: Life cycle’s personal (data, program, traces) entities Security (security issues)***Medium-Term*

- Each individual creates and manages the lifecycle of their personal data, which are shared and controlled by others entities through the network.

⇒ **Dedicated overlay paradigms; garbage collector on the network to (securely) clean up the personal data**

**7.2.3 Goal 3: Security policies between massive, participating & competitive actors***Short-Term*

- Mutual security infrastructure, shared between competing operators (Telecom Operators, Network providers, Service/content providers, etc.)

⇒ **Virtualization: packets, routers, channels, bandwidth, session ...**

*Medium-Term*

- Re-equilibrium of the unfair and unequal face-to-face relationship of the end-user in front of the network.
- Governance of the infospheres of people: scalability over vast populations; traceability, log data management; accountability management.

**7.3 Cloud computing & Nomadicity cross-topics**

The following are topics which are cross-linked within the use cases examined by WG1:

- Interoperability of policies;
- Accountability and presentation/usability;
- Standards and platform-independence, (open platforms for all entities?)

**7.4 e-Health****7.4.1 Short-term challenges**

1. Define who the stakeholders are within the e-Health eco-system:

- Patient-centric strategy – *centric* meaning “control, responsibilities, rights and duties”
- Re-focus e-Health from a “*security and fraud reduction*” approach to a “*Privacy and Trust*” approach, implying a need for the extension to new players outside current systems; for example, forums, social networks, e-Health advisory services, etc.

## 2. Data (Patient Health Records - PHRs) storage and responsibilities strategy:

- Where is the data stored?
  - Keep in mind #1: 100% of the population has to be served.
  - Keep in mind #2: This can't be limited to one option.
- Access and retention issues: Who? What for? When? And, for how long?
- Rules for data retention and third parties access
- Policies to clearly define the do(s) and don't(s), regarding:
  - Transactions
  - Edits to PHRs

## 3. Define the Control Authority within the eco-system:

- Split the role of security enforcement and privacy assurance.
- Define "patients' rights and duties".
- Educate the actors in the eco-system
- Auto-enforced rules?

### 7.4.2 Medium-term challenges

#### 1. Define the tools (privacy UI and support) for users to control and parameterise their PHR life cycle:

- Realise Patients' rights and duties via actual tools, preferably platforms-agnostic
- Educate the stakeholders/actors about policies and their consequences

#### 2. Implement a method of delegation of authority for all PHRs access control rights and duties:

- For people who need sudden (or planned) assistance
- To enable access to care services for 100% of the population (regardless of education and resources to access to ICT-Based systems)

#### 3. Implement a method for opting-out Patients' PHR for stakeholders with statistical needs for data:

- For broad health programmes (epidemic, etc.)
- To complete a comprehensive data life cycle strategy

## 7.5 Identity Management for eGovernment

### 7.5.1 Short term challenges

#### 1. Multiple identities environment:

- Supported by state/government
- Clear definition of controls, rights, responsibilities
- Dynamically user-created identities
- Who will enforce? - Government?

#### 2. Peer-to-peer e-ID authentication among citizens:

- Keep the function of “classic” ID cards to enable authentication among citizens without having to ask for government support in each case
- Infrastructure required
- Could enable private use of e-ID infrastructure
- Can readers be deployed to read passports/ID cards with consent?

### 3. Privacy implications of multiple identities

- Credential definitions can be slim – just fitting the applications and privacy requirements but can also be overly broad
- Help with tools to find a balance

## 7.5.2 Medium term challenges

### 1. Building upon which issuing party approach gives trustworthy identities/identifiers?

- Credentials coming from multiple identity sources:
  - e-Gov central based approach (top-down)
  - e-Gov local based approach (rather bottom up)
  - Peer-to-peer (social networks, private parties) approach (bottom-up)
  - Combination of top-down and bottom-up approaches

### 2. Market for e-ID platforms

- To place Identifying credentials on different platforms
- Users can switch from one to another if not happy
- Economic value of secondary usages

### 3. e-ID/PETs integration

- The need for PETs will become apparent with expanded use of IT for identification
- Uptake of PETs will happen with integration to development

## 7.6 e-Health & e-ID cross-topics

There are a number of issues relevant to both of the use cases discussed by WG2:

- Data storage and responsibility strategy
- Start with straightforward, simpler use cases and then progress to more *in vivo* cases
- Role separation:
  - Multiple roles in digital life; for example, one professional and one private
  - Being un-linkable should be an option
- Multiple stakeholder definitions and relations regarding control, rights, responsibilities, trust relations, etc.

## 8 Summary of Overall Conclusions

Taking as given the general statement of the needs for trust and security, a number of fundamental areas were identified. The conclusions are summarised in two groups below: the first mainly from the user standpoint, with the second looking at means of supporting the users' needs. This outcome corresponds well with the scope of the two Working Groups.

Updated [use case documents](#), based on the discussions which took place during the workshop, are available on the Think-Trust web portal. (*Access to these documents requires log-in to the Members Area*)

### 8.1 User-centricity: WG2-related

Typified by e-Health, as a high-demand instance – putting the user at the centre of considerations, with rights, duties, responsibilities, and controls, and the problems of provision and management of user identity:

- Privacy: protection of all aspects of 'me'
  - Identity-related, location and time, my data, and what I do, in conformance with agreed policy;

(*Note: There may be non-negotiable elements – “I cannot by law forfeit or deny certain rights and duties”*)

- Measures to control profile aggregation, to avoid and also to clean-up the detritus in the wake of our activities, plus regulatory controls to outlaw intrusive practices.
- Data-protection: clear responsibilities for data-controllers
  - Responsibilities and liabilities;
  - How and where data is stored and handled, and what is permissible (authorised?) use of user-data – what actions and by whom (includes delegation), together with effective controls

#### 8.1.1 Identities and Identity Management

Identity lies at the heart of trust and security requirements and issues. It also lies at heart of the solutions to satisfy these issues. In addition to identities of, or attached to, humans and their organisations, all entities, real and virtual, in the digital environment must be covered – *naming* and *addressing*, but in new dimensions. Identity and identification need to be globally usable, and to interwork at several levels.

The requirement is for a framework for identity provision/creation, handling and usage that supports interoperability between different regional or cultural domains:

- Identity provision and global mutual recognition between administrations: *official* identities, organisation-related identities and roles, personal (cf nick-names) and ad-hoc/temporary/one-time IDs or aliases;
- Management and use of complex/fragmentary/partial identities, including roles, and anonymity and pseudonymity within certain limits that respect privacy and freedom of expression but restrict damage to innocent individuals and groups, and subversion of society and nation.

Kim Cameron's [Laws of Identity](#) provide guiding principles to how identity is to be protected and respected.

### 8.1.2 Privacy and Data Protection

A fundamental right, recognised in European law and tradition, is the respect and protection of privacy in terms of information about or relating to the individual, together with the data that belongs to the individual. Many high-profile instances of disclosure have been incompetence – *human error* – but there are many instances of active malfeasance (even if some may ultimately be in the public interest). Legislation is all already in place and is being further developed such that it establishes responsibilities for those in charge of information; but tools and facilities are required that will enable *data controllers* to discharge their duties properly. Further policy and technical measures are needed to combat the covert amassing of information relating to individuals and groups – profiling, aggregation, data-mining and crawling, etc. – both before and after the act: possibly to outlaw and prevent the extraction of information but also sweeping up personal detritus that may be disclosed or discarded in ignorance.

### 8.1.3 Use of Services

The user needs access to services that provide a proper mutual balance of transparency and accountability with respect to rights and duties: at present, a balance that appears in favour of the service provider. For example, <I **accept**> – **click!** In practice access is going to be much more complex and dynamic than is currently the case, and hence a framework is needed that will provide for the performance, in real time, of the agreed terms of the relationship between service and user (client). The user wants to be able to trust what is happening with (their) information, and how agreed duties of care are discharged, even though there will be discontinuities, change of device, change of location, etc.

### 8.1.4 User support and orientation

The complexities of how security facilities and mechanisms are to operate are beyond the comprehension and capabilities of all but a handful of experts. Some form of automation, provided by helpful interfaces, tools and off-the-peg profiles, is needed that will allow the user to make sensible decisions to suit personal circumstances and preferences. But to make sensible decisions, even if only to select some typical, standard profile, there is still the need for awareness by the user of what is going on, what are the risks protected against, etc. Therefore, some awareness programme or **Help** facility should be available, providing a wide range of support and advice from the ICT naïve to the reckless know-all. This will require close cooperation between the technology designers and ergonomic and usability experts.

## 8.2 Security, Privacy, Trust, and Dependability

This section looks at what is needed to support the nomadic, mobile user, and to enable the trusted use of Cloud-based services. A number of key characteristics and requirements are identified, together with an indication of possible regulatory support.

### 8.2.1 Architecture for Trust and Security

The requirement is for a frame of reference that establishes what are the components, and how do they relate and interact, how do they compose, and how are boundaries, regions (domains) established and regulated: how does it work (correctly) and what happens when it malfunctions. The reference framework needs to support the design and specification, modelling, implementation, and operation and monitoring of the system. The emphasis is on the interoperability of all aspects of trust and security, and therefore there is a need for standards to describe heterogeneous entities and express the dynamic relationships between them.

### 8.2.2 Virtualisation

As the physical boundaries dissolve and blur, new virtual separations and boundaries must still be established and maintained; virtualisation and the mapping of constructs to physical resources must be developed and extended. Compartmentalisation provides a means of isolating and protecting areas of trust, and controlling relationships with other areas. It also supports the simplification of complex structures into foreseeable, manageable components.

### 8.2.3 Accountability

There may appear to be tension or conflict between Accountability and Privacy; thus, accountability must be privacy-respecting. Engineered properly, it does in fact support privacy by, for example, providing the ability to trace accidental, incompetent, or malicious access to personal information (both *owned-by* and *about*), and working with properly protected identity in defending against wrong allocation of responsibility. Robust accountability is also seen as a deterrent against unauthorised intrusion – malicious or accidental; however, this must be in conjunction with, rather than instead of, access controls based on strong identification.

### 8.2.4 Interoperability

A specific need for automated (security) policy governance was identified. This governance extends from the formulation and agreement of what is to be provided with respect to aspects of trust, privacy and security, through the monitoring and reporting conformance of operations, and on to the remedial action for non-compliance. The arena for all this is again the generalised, mobile, polymorphic dynamic environment – but without burdensome operational overhead.

However, it appears that this may have common characteristics that are ‘typical’ of a number of basic *functions*, which are required to operate across a range of services and entities. (Are these common characteristics in fact aspects of policy agreement? For example, agreement between entities about their relationship? How to handle detailed aspects of, say, accountability, data protection, privacy, etc.

### 8.2.5 Technologies and Engineering to support multi-level security and assurance

The underlying security technologies and techniques need to progress so that they keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment outlined above.

- Cryptography: fast, cheap, *light*, (low power, ease of use and support, etc.);
- Trusted execution (environment) – how else do we know that what is supposed to happen really does happen;
- Trustworthy functionality – SW and HW; how to design, produce, and assure trustworthy components, and how to build them into larger trusted entities and assemblages? This calls for tools (themselves trustworthy) and ‘criteria’ that will support the policy governance outlined above. The technology needs a platform-independent dimension to allow for interoperability of trusted entities – in addition to the security aspects of trustworthiness, we need to address the wider issues of quality and dependability;
- Measurement and metrics – related to the previous item – we need to be able to measure aspects of trustworthiness, and to articulate and quantify the *dimensions* and units; this is required in the wider field of assessment of trust/risk and security/vulnerability;
- Basic engineering: we need to weigh up the considerations of cost and economics, power and energy *versus* strength, performance and functionality;

- Education, Training, and Awareness: in addition to the general user help and support, above, there need to be standards for professional training and proficiency, and the tools and methodologies for the designers and engineers to build and maintain the future networks.

## Annex 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:

1. 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/risseptis.html>
2. To establish and support Working Groups of multi-disciplinary experts that will provide technical input to the generation of the RISEPTIS report.

### 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.

## Annex 2 – Workshop participants

Caspar Bowden	Microsoft	WG2
Jim Clarke	Waterford Institute of Technology ( <i>P</i> )	WG2
Brian Foley	Waterford Institute of Technology ( <i>P</i> )	WG2
Keith Howker	Waterford Institute of Technology ( <i>P</i> )	WG1
Erland Jonsson	Chalmers University of Technology	WG2
Sokratis Katsikas	University of Piraeus	WG2
Paul Koster	Philips Research	WG2
Xavier Larduinat	Gelmato	WG2
Herbert Leitold	Inst. for App. Info Processing and Comms	WG2
Fabio Martinelli	National Research Council of Italy	WG1
Svetla Nikova	Technische Universität Twente	WG1
Kieron O'Hara	University of Southampton	WG2
Aljosa Pasic	ATOS Origin	WG1
Sachar Paulus	Paulus Consulting	WG1
Kai Rannenber	Goethe University Frankfurt	WG2
Sathya Rao	Telcom ( <i>P</i> )	WG1
Michel Riguidel	ENST ( <i>P</i> )	WG1
Mary Rundle	Oxford Internet Institute	WG2
Amardeo Sarma	NEC Laboratories	WG2
Jan Schallaboeck	Independent Centre for Privacy Protection	WG1
Dieter Sommer	IBM Research	WG2
Kieran Sullivan	Waterford Institute of Technology ( <i>P</i> )	WG2
Neeraj Suri	Technische Universität Darmstadt ( <i>P</i> )	WG2
Mike Surrige	University of Southampton	WG1
Elena Troubitsyna	Abo Akademi University	WG1
David Wright	Trilateral Research & Consulting	WG2

*(P) – Project Participant*

### Invited Speaker

Maria Veronica Perez Asinari      Office of the European Data Protection Supervisor

### Commission/Reviewers

Eleni Christodoulou      University of Cyprus  
Udo Helmbrecht      BSI Germany  
Thomas Skordas      European Commission

## Annex 3 – Workshop Agenda

The agenda was proposed to give maximum time for the Working Groups to address the Use Cases.

	START	DURATION	DISCUSSION ITEM
<b>Day 1</b>			
<b>Plenary</b>	<b>09:00</b>	<i>0:30</i>	<b>Introduction, agenda, goals</b>
<b>Plenary</b>	<b>09:30</b>	<i>0:25</i>	“Current EU thinking on Data Protection” (Maria Veronica Perez Asinari, EDPS)
<b>Groups</b>	<b>10:15</b>	<i>2:00</i>	Session 1 – Use Case Scenarios: Review and Discussions
<b>Groups</b>	<b>13:15</b>	<i>2:15</i>	Session 2 - Development of 2015 Scenarios
<b>Groups</b>	<b>15:50</b>	<i>2:00</i>	Session 3 - Identify challenges per WG
<b>Plenary</b>	<b>17:50</b>	<i>0:15</i>	<b>Wrap up of the Day – conclusions, guidelines for Day 2</b>
<b>Day 2</b>			
<b>Groups</b>	<b>09:00</b>	<i>1:30</i>	Session 4 - Refinement and consolidation of challenges and priorities in WGs
<b>Plenary</b>	<b>10:30</b>	<i>2:00</i>	<b>Present group findings – consolidation, conclusions, priorities</b>