

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

D3.2 Public Consultation Report

Start date of project: 1st January 2008

Duration: 30 months

Organisation name of lead contractor for this deliverable

Waterford Institute of Technology

1. Introduction

The development and growth of the Information Society is driving ICT advancements forward at ever-increasing speeds, resulting in a dynamic, fast-changing and cross-dimensional environment. In this period of rapid growth and change, there is a strong and urgent requirement to develop “smart” (meaning intelligent, user-friendly and user-centric) ICT security environments that take full and simultaneous account of:

- Freedom of access, interaction and use;
- Respect for privacy within society;
- Security and dependability.

The ultimate objective is to develop a framework which enables a sustainable balance between these factors while strengthening the security of the digital environment and enhancing its privacy, dependability and trustworthiness.

The Think-Trust Project (www.think-trust.eu) has initiated a series of actions that contribute to this goal. The project, an EU FP7 co-ordination action (CA) will examine the needs of the supplier and the large user while also incorporating the perspectives of the citizen and their ICT interactions with technologies, services and goods.

The Project is mapping and modelling new ICT environments with the specific goals of:

- Defining new areas of work in ICT Security Research;
- Furthering the EU's strategic thinking and positioning in the field;
- Influencing ICT technology developments in the coming years.

The project is addressing a broad spectrum of interests and drivers. The span of non-technology sectors, the technology coverage, communications, end-systems, applications and services must all be taken into account. The structures and working methods of the project allow a broad range of ideas to be aired, ranging from concerns about protecting the end users and their assets, to issues such as securing and protecting large, polymorphic ICT network and service infrastructures and underlying practices.

One of the key objectives for the project is to formulate **Recommendations** on the:

- **Policy environment** – the development of coherent legal and administrative frameworks, operational environments and human behaviour relating to security, privacy and confidence, in view of the technological changes leading to and arising from the future Information Society,
- **Research Agenda** – Future European research and development that can facilitate the creation of an Information Society that will be secure, whilst respecting freedom and privacy of its citizens, with due attention given to the ICT infrastructures, networks, services and applications.

The Think-Trust project will deliver an analysis and recommendations for future actions, including necessary supporting research, which will lead to the availability of balanced, appropriate levels of trust, security, and dependability to support the envisaged ambient, digital environments.

The expected final results of the Think-Trust project include a more explicit understanding of the trust, security, privacy and dependability challenges relevant to ICT stakeholders in the Information Society, as well as a heightened awareness of these aspects among the wider European technological community in the next 5-10 years timeframe. The recommendations in the areas of future ICT security policies and research agenda will have a significant bearing on: the confidence levels of users; ensuring that Europe is well-positioned to embrace ICT developments; and, finding the correct balance between the social, legal and technical requirements in future Information Society to address security, privacy and dependability.

2. Interim Research Recommendations

An interim set of research recommendations concerning the main challenges and key research priorities in the area of **Trust, Security** and **Dependability** have been identified in Deliverable 3.1a ([click here](#)). The Deliverable sets out the scope of the challenge of providing Trust and Security in a new age of information processing in daily tasks, and a vision that identifies the areas where research, development and deployment of technologies will be necessary.

The deliverable which is closely aligned with the RISEPTIS report and the outcomes of the two Working Group plenary workshops, elaborates in more detail the four research priorities identified in the RISEPTIS report, viz:

1. Security in (heterogeneous) networked, service and computing environments
2. Trust, Privacy and Identity Management (metasystems) Infrastructures
3. Underpinning Engineering Principles and Architectures that support Transparency / Accountability Architectures and Measurement
4. Data, Policy Governance and Socio-Economic aspects

The Deliverable was further refined in the period with the publication of [D3.1b](#). This was a more concentrated document and, based on the four priority areas identified by recommendation 1 of the RISEPTIS Report, detailed the key research challenges that require attention in order to provide trustworthy hardware and software for the Information Society. The research challenges identified also take account of the wider landscape as identified in the Working Group discussions, FIA outputs, etc.), as well as recognising the topics already covered in previous calls (up to Call 5).

Deliverable 3.1b identified research challenges in the following areas:

- **Trust ‘engineering’**

Trust is not absolute and will be quantified by the preferences and intuitive policies of users. This gives rise to the need for an overall *trust framework* (rather than a *security framework* per se), where trust-relationships between entities are established and managed to encompass trust ‘preferences’, trust ‘policy’ and trust ‘weighting’.

- **Quantification of trust, security and privacy**

A better quantification model is needed than is currently in place. Investment in experimental setups and test-frameworks that can be thoroughly measured in terms of security would advance this process.

- **Architecture**

In general, architectural support must be provided first with regard to transparency – security monitoring, observability and measurability for data logging and log access – and secondly, with regard to the ability to function across multiple layers and domains, as well as having policy awareness and transparency as architectural properties.

- **Cyber-security: Engineering and Technology**

Techniques and mechanisms to provide protection, assurance and integrity are required. These must keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment. Such tools should be robust and resistant to failure and attack (survivability). As well as these tools, criteria and standards to support policy governance is also required.

- **Accountability**

There will always be faults, failures, mistakes and attacks. Accountability is a research priority, as it creates the means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress.

- **E-Identity**

RISEPTIS recommendation 3 calls for the development of a common EU framework for identity and authentication. It is recognised that there will not be a single, unified format or scheme for eIDs, and that there will be multiple national or regional and commercial eID domains. There is also broad consensus on the need for flexible identity systems where users might have an *à la carte* choice (as an aspect of user-centricity) regarding identity-data options.

- **Privacy**

Objectively verifiable data was previously compiled and managed for specific and acknowledged purposes. Now, however, data-gathering systems operate greedily and indiscriminately, grabbing data from each and every source. This opens up new possibilities for tracing, monitoring, shadowing and digital inquisition, with the possibility of registering and following every move of every object and processing and cross-referencing this data.

- **Protection**

Related to Privacy (including business confidentiality), the protection of data processing, storage and transmission, as well as the shielding of resources and assets (information, services, devices, communications) require: compartmentalisation; fine granularity access control; mutual authentication; new cryptographic techniques in preparation for the quantum/post-quantum age; uses of eID to assist in data protection.

- **Usability**

The Future Internet, and more generally, tomorrow's communication networks will be focussed squarely on the individual (the citizen, the end user, the consumer). The aim of all future R&D programmes will be to influence the nature and scope of this central position. Making usability a permanent requirement of engineering would be a step in the right direction when addressing this challenge.

- **Management and Governance**

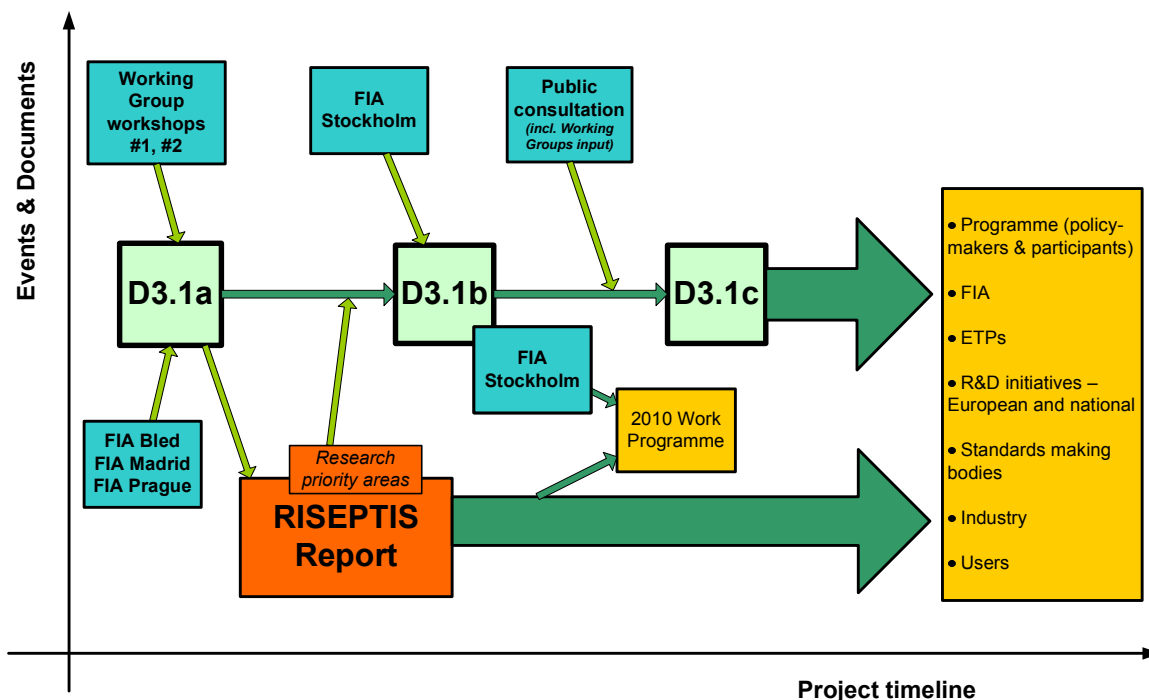
The proper management and operation of security policies must be considered in the context of the environment in which they operate. These settings could be ambient, heterogeneous, volatile, etc. Continuity of security relationships within these dynamic environments must also be appropriately managed.

- **Socio-economic**

RISEPTIS Recommendation 2 calls for convergence of technology with other areas and disciplines; Recommendations 3 to 6 contain specific requirements for parallel advances in non-technological areas.

3. Public Consultation Process

A Public Consultation Process forms a key part of the process in ensuring that the wider security community have an opportunity to comment on the interim research challenges identified in the project. An overview of the process of developing the research challenges is outlined in diagram 1 below.



As can be seen in the above diagram the project's [Public Consultation process](#) will play an important part in securing additional inputs from the wider security community to feed into the development of D3.1C Research Recommendations (final) due for publication in June 2010.

The Public Consultation Process was officially launched on October 7th, at the FIA 'Trust and Identity' Caretakers' Workshop. At this event, the Think-Trust interim research recommendations were presented to a cross-section of experts from the domains of 'Networks', 'Future Content', 'Service Platforms', 'Service Infrastructure' and 'Identity & Privacy'.

This initial launch was followed up with announcement in the project's website ([click here](#)) and newsletter ([click here](#))

Posters (annex) announcing the public consultation process were also displayed at the [FIA Stockholm](#) event, designed to make the wider trust and security community aware of the interim recommendations from the project and making them aware of the opportunities to input. A similar poster was also announced at the [Irish Future Internet Forum](#) event which took place on December 3rd, 2009, in Dublin, Ireland. This event was attended by a wide range of researchers from academia and industry and included key notes from Conor Lenihan, TD, the Irish Minister of State for Science, Technology, Innovation & Natural Resources and Mr. Jacques Bus, Head of Unit 'Trust & Security in ICT Research'.

It is also planned that some of the key note speakers at the in Trustworthy ICT event in Leon (<https://trustworthyict.inteco.es/>) on 10 and 11 February will make the participants aware of the process.

An intensive effort to engage the widest possible involvement will be undertaken in February 2010. For this purpose a questionnaire has been developed which will be circulated widely.

4. Questionnaire

4.1.1. Introduction

The Think-Trust project has identified an interim set of research challenges that require attention in order to provide trustworthy¹ hardware and software for the Information Society. These research challenges stem from the four priority areas identified in Recommendation 1 of the RISEPTIS Report ([click here](#)).

- Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet
- Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability
- Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography)
- Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management

We are now seeking input on these interim research challenges from the wider trust and security communities. For further details on these research challenges, please see Deliverable 3.1B (Interim Recommendations Report) on the Think-Trust website ([click here](#)).

If you would like to have your opinion heard, please score the identified research challenges in this questionnaire

(Completion of this questionnaire should take no more than 15 minutes)

The feedback received during this public consultation process will contribute to the final Think-Trust Recommendations Report (D3.1C), due for publication in June, 2010.

Responses by Monday, March 1st, 2010

Paper: **Kieran Sullivan**
 TSSG
 ArcLabs Research and Innovation Centre
 Waterford Institute of Technology
 West Campus
 Carriganore
 Waterford
 IRELAND.

Electronic: consultation@think-trust.eu

¹ For the purposes of this questionnaire, trust and security covers a broad spectrum that includes the trusted use of (and trust in) communications and services; privacy and protection of personal and commercially sensitive information; and protection of services and infrastructure (cyberspace).

4.1.2. Questionnaire

Please assign one of the following scores to the challenges identified.

- A*** absolutely mandatory for progress from current position
- A** essential to provision of trust and security for Future Internet and the Information Society
- B** necessary to achieve broad usability and uptake
- C** required longer-term response to new technologies and potential threats
- D** required for provision of attractive and competitive services
- X** not necessary or not urgent

RESPONDENT NAME (OPTIONAL)	ORGANISATION	E-MAIL ADDRESS

	Comment	Score
Trust 'engineering'		
Development of overall <i>framework for trust</i>		
Support trust relationships (establishment, management, and maintenance)		
Development, expression and use of trust indicators;		
Automatic computation of trust assertions, based on policy frameworks that take into account user preferences;		
Life-cycle management, including maintenance, repair and recovery;		
Models, methodologies, measurement of trust (see Quantification below);		
Tools to calculate it (a combination of assisting the user and quantifying personal trust);		
Assessment of availability / downtime / integrity / confidentiality to feed into trust models		
Delegation and acceptance of trust and privileges.		
Quantification of trust, security and privacy		
Scaling results on trust experiments from the laboratory environment to the real worlds of the Future Internet?		
Generalisation of security predictions across different software components, programming languages, systems, environments?		
Collection and sharing of security-related data for experimental research		
Architecture		
Policy awareness and transparency as architectural properties		
Transparency support : monitoring; observability; logging, accessibility		
Consistency of security and trust facilities and mechanisms across layers and domains		

	Comment	Score
Meta architecture –higher-level abstractions to help structure a global information security architecture?		
Network and service architectures – scalability and interoperability of the current architecture consider service composition/aggregation)		
Damage control: domains, partitioning, compartmentalisation in (e.g.) Cloud environment, including dynamic service composition/aggregation		
Architectural standards (to support) <ul style="list-style-type: none"> • pre-conditions for interoperability; • verification of conformance requirements; • built-in emergency measures; • establish workable definitions concept (metadata, ontologies, etc.); • support for security policy management, including the ability to attach policy information to data. 		
Cyber-security: Engineering and Technology		
Techniques and mechanisms to provide protection, assurance and integrity		
Robustness, resilience, survivability		
Criteria and standards to support policy governance		
Interoperability, and platform independence		
Virtualisation to support construction of complex concepts such as high-demand, critical services on otherwise limited technologies		
Security in environments with scarce resources		
Support for legal policies and requirements		
Tools and technologies to support design and construction of future trusted environments and networks		
Accountability		
Means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress		
Interoperable, robust accountability framework: that balances privacy and traceability; that is economically feasible; that protects against non-repudiation but also against incorrect attribution		
Consistent interpretation of security policy agreements; appropriate standards for protocols and interfaces, and for tools to enable compliant usage		
Traceability and accountability on global accountancy-type principles		
Territorialisation of (trace/log) information; local domain policies and management; restricted ‘sharing’ only with authorised participating domains		
Real-time, large-scale test-beds to generate confidence (related)		
Applicability to charging and payment		
Anonymous/pseudonymous charging and payment systems		
Anonymization or impersonation tools to produce untraceable, but trustworthy, valid sources/channels for eg, provision of economic, social, or health statistics		

	Comment	Score
E-Identity		
Common EU framework for identity and authentication		
Interoperability of/with alternative (and current) ID schemes		
Flexibility of choice of identity and ID-protection options/choices, including partial IDs and anonymity when appropriate		
Life-cycle management of IDs, with protection recovery from loss or failure		
Standardised linkages to related and dependent concepts (accountability, access-control, etc.)		
Claim-based approaches using novel and existing cryptographic protocols to eventually avoid ID architectures with a centralised components that everyone needs to trust		
Technology to support new business models for central, decentralised, and claim-based approaches		
Communication setup and routing that are identity-data-aware only as necessary for network functions, without making the related users identifiable or traceable		
Privacy		
Minimisation of unintended acquisition of personal and other sensitive information		
Fine granularity access control to identity-related information		
Further development of Privacy Enhancing Technologies (PETs); tools to check privacy assurance and tools to advance transparency regarding used data		
Use of policy-based automated controls to manage the entire lifecycle of personal data in accordance with the dynamic needs of the data subject and the data users		
Methods for capturing detailed personal consents and preferences/requirements, representing these and rigorously managing their subsequent evolution, including revocation/retraction		
Possibility to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates		
Personal/communal collector of personal garbage/litter (or timed auto-self-destruct)		
Use and control of identity-related information for network (e.g. routing) purposes without compromising privacy (see 0, above)		
Standardised techniques to assure privacy across the various internet layers, through to network level and maintaining consistent privacy across different environments		
Tools and concepts for deleting data in the internet ("forgetting") – see 0, above		
Protection		
Related to Privacy, above, plus confidentiality and integrity for business/administrations		
Protection of data processing, storage and transmission, as well as the shielding of resources and assets (information, services, devices, communications)		
Domains, partitioning, compartmentalisation, fire-breaks – leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localisation of damage		

	Comment	Score
Fine granularity access control based on multiple bases for authentication and authorisation. For example, IDs, privileges, roles, etc		
Mutual authentication, with multiple devices (ideally, technology invariant)		
New cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age		
Uses of eID and its components in protecting the interests of its subject (data protection, etc.)		
Usability		
Support for the individual user (user-centricity)		
Environment can adapt to user choice as well as presenting auto-configurations based on assumptions and profiles, depending on levels of (user) trust (of environment)		
What does the user want or need by way of security and trust facilities and functionality? (including non-technical, human aspects) - how is this delivered		
What are the impacts and implications for the underlying mechanisms and functionality		
Attention to user/system interaction: sympathetic user interfaces, but with advanced options		
Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms; this may include decision support, recommended options, and the capturing of user preferences (profile).		
Management and Governance		
Framework for consistent expression and interpretation of security policies, and the means of and implementing policy intentions at all levels, from network layers up to business and legal needs		
Investigation of economic feasibility and possible alternatives		
Technical support for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions; at a simpler level, the regulatory aspects to support the interoperability of security policies are necessary: from civil law for individuals and society, and contract law for business, to <i>common law</i> and the support of small claims		
The relationships between eIDs and Government (.gov) must be given special attention – registrations, births, marriages, deaths, etc.		
Socio-economic		
Convergence and coordination of technology with other areas and disciplines, with parallel advances in non-technological areas		
Explore role of other areas of business/industry should be examined to learn how they handle security/risk-analysis, eg, can the insurance industry balance risk and cost for different categories of users? with formal certification of trustworthy products/services and the classification of users, and no-claims discounts, additional premiums for risky use, exclusions, etc		

	Comment	Score
Analysis of economics and inertia in the market place – why has security and trust been undervalued? – but possibly need to approach via the cost of insecurity; and user-perception of value of trust and security versus goodies and add-ons		
Incorporation of EU legal framework, for all jurisdictions currently covered, together with new laws and regulatory measures as necessary		
Constant engineering vigilance about economic viability: is it more cost-effective to (generically) prevent a data breach or just address the consequent (case-by-case) damage after the event		
Exploration of market place and related drivers for eID management (and other security and protection) - to place Identifying credentials on different platforms - user-choice of ID 'home' - economic value of secondary usages		

Overall coverage (free text)

- Are there additional topics that need to be added to the interim list above?
- What topics need to be amplified or extended?
- Should any topics be removed, down-graded, or postponed?

Context and Overall Landscape

Please indicate your assessment of the importance of the listed items below:

	Comment	Score
Trends		
Increased, heterogeneous accessibility to converged information and services. (For example, ubiquitous, mobile access, very high bandwidth fixed networks and access)		
Increasing volume of transactions, and even higher volume of traffic		
Large growth of sensors and slave-labour devices (<i>Internet of Things</i>), taking over the management of routine operations in commerce, utilities, the environment, and law enforcement and security provision		
Increasing mobility of users (physical or virtual), seeking either continuous (mobile) or intermittent (nomadic) connection and access to information and services		
Convergence of types: voice, visual, entertainment, social and business services. (eg, twitter.gov, and 'official' blogs)		
<i>Nano</i> to <i>mega</i> computing and communication – from cheap, incoherent, tiny, low-resource entities in massive numbers handling the routine, to the gigantic cooperative high-resource super-grids addressing the difficult and complex		
Existing threats, vulnerabilities, risks		
<i>defects and failure/damage opportunities of the current Internet</i>		
Fragility – networks and end-systems are vulnerable to simple attack, with information easily accessed, destroyed, copied and stolen, or falsified		
Software subject to design, implementation and usage errors, (hardware is not faultless, but more easily verified during design)		
Domino effect across inter-dependent systems in the case of accidental malfunction and/or failure, and attack propagation		
Unprotected networked data exchange, but also via external media		
Lack of user-awareness regarding their data, together with difficulties in understanding and availing of privacy-providing tools. the burden to the user in using these often complex tools hinders their acceptance and uptake		
Basic usable security and trust facilities that enable the user to make informed choices or decisions		
<i>some malicious specifics</i>		
Fraud – breach of enterprise records/systems, stolen/captured credit card and bank details		
Intrusion – Trojans: key-logging; colonisation, 'hacking'		
Impersonation through identification theft or failure		
<i>Phishing</i> etc. relying on deception (spoofing) of user		
Identity profiling from digital trails		
Unauthorised disclosure: 'inside jobs' (police, government agencies, etc. for press and private investigators)		
Malware – viruses, worms, etc., for vandalism or		

	Comment	Score
blackmail/ransom threats		
IPR abuse – unauthorised file sharing, plagiarism		
<i>Denial-of-service</i> attacks		
Unjustified trust – use of the 'open' net for sensitive operations (own goals)		
Defence-related – internet gateways to 'secure' systems		
Emergency services		
Utilities management		
Health systems		
Financial/economic systems		
New threats, vulnerabilities, risks		
New architectures will include structures and protocols that blur boundaries between: <ul style="list-style-type: none"> • what previously would be identifiable as domains (of, say, responsibility or control); • real, logical, and virtual domains; • where functionality actually lies – in hardware, in software, in the network, in information itself; • what is an application and what is a service 		
need for new architecture (as a whole) to pay attention to its own security needs and implications, as well as those of its <i>clients</i>		
vulnerabilities from the increasing integration of services, and avalanching failure		
total penetration of our lives, and consequent danger of the diminution and dilution of personal privacy and sovereignty (and that of enterprises or even administrations)		
the possibility of multiple <i>big-brothers</i> watching, recording, and analysing our actions		
need for non-expert user to be informed, and to make appropriate decisions – in many cases, < I ACCEPT> the informed default advice from the "security" interface		
FIA directions		
(the following are 'givens', but state your ranking in any case)		
Management and Service-aware Networking Architectures		
Services and Software (platforms and infrastructures		
Content Creation and Media Delivery		
Trust and Identity		
Internet of Things		
Real world Internet		
Future Internet Research and Experimentation		
Future Internet Socio-Economics		

Annex A - Background Information: Extracts from D3.1B

Research & Development Challenges

A1.1 Summary Think-Trust Recommendations

Trust 'engineering'

The lack of trust in ICT infrastructures (including entities, actors, service providers) shows itself during *operation* (because systems must confront intentional attacks or cope with accidental breakdowns), and at the *design* stage (because security or resilience are often not included in the system's specifications). Trust is not absolute and will be quantified by the preferences and intuitive policies of users. This gives rise to the need for an overall *trust framework* (rather than a *security framework* per se), where trust-relationships between entities are established and managed to encompass trust 'preferences', trust 'policy' and trust 'weighting'. This would include:

- development, expression and use of trust indicators;
- automatic computation of trust assertions based on policy frameworks that take into account user preferences;
- life-cycle management, including maintenance, repair and recovery;
- models, methodologies, measurement of trust;
 - tools to assist users calculate it (a combination of assisting the user and quantifying personal trust);
 - to assess availability/downtime/integrity/confidentiality to feed into trust models
- delegation and acceptance.

Alternative approaches should also be explored, including more complex social controls in the virtual world, including *reputation*, *recommendation*, *frequentation*, *voting*, *gaming*, etc. approaches.

Quantification of trust, security and privacy

Advances in the insurance analogy (see 4.10) can only happen if we change how we look at the security level of systems. We need a better quantification model. Investment in experimental setups and test-frameworks that can be thoroughly measured in terms of security would advance this process. This would also allow the following question sets to be examined:

- Do results on trust experiments scale from the laboratory environment to the real worlds of the Future Internet?
- Can security predictions be generalised across different software components, programming languages, systems, environments?
- How do we collect and share security-related data for experimental research in the line of the work presented?

Architecture

In general, architectural support must be provided first with regard to transparency – security monitoring, observability and measurability for data logging and log access – and secondly, with regard to the ability to function across multiple layers and domains, as well as having policy awareness and transparency as architectural properties. There are a number of aspects to these architectural challenges:

- *meta* architecture – would higher-level abstractions help to structure a global information security architecture?
- *network* and *service* architectures – examine the scalability and interoperability of the current architecture and consider domains, partitioning, compartmentalisation in a Cloud environment (including dynamic service composition/aggregation)
- architectural *standards*
 - pre-conditions for interoperability;
 - verification of conformance requirements;
 - built-in emergency measures;
 - establish workable definitions concept (metadata, ontologies, etc.);
 - support for security policy management, including the ability to attach policy information to data.

A core question in this section is the “functionalisation” of security properties: wherever we are able to functionalise, we can improve the acceptance of security. Therefore, we need to ask, how can this be done in a systematic way? *Security patterns* provide a first approach, but this needs more systematic management.

Cyber-security: Engineering and Technology

Techniques and mechanisms to provide protection, assurance and integrity are required. These must keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment. Such tools should be robust and resistant to failure and attack (survivability). As well as these tools, criteria and standards to support policy governance is also required. Technologies need a platform-independent dimension to allow for interoperability of trusted entities.

- Virtualisation should be examined in this regard, since it allows complex concepts such as high-demand, critical services, to be built on top of limited technologies.
- Security in the presence of scarce resources must also be considered:
 - self-organised and other self-* ubiquitous computing systems
 - sensor networks – adaptive and able to aggregate data
- Legal domains with different priorities: how to address in a virtualised scenario? Technology is needed to support this “dynamic switch of security controls” based on legal policies.
- Education, Training, and Awareness: in addition to the general user help and support there is a requirement for standards for professional training and proficiency, and the tools and methodologies for the designers and engineers to build and maintain the future networks. (Close relationships with established CERT² teams and ENISA³ would be of added benefit to this goal.)

Accountability

There will always be faults, failures, mistakes and attacks. Accountability is a research priority, as it creates the means to establish responsibilities and liabilities and the basis for investigation, sanctions, restitution and redress.

There are two options which seem especially promising and coherent:

² <http://www.cert.org>

³ <http://www.enisa.europa.eu>

- Base the demand for traceability and accountability on global accountancy-type principles, which can encompass the whole network, and such that reliable and finely granulated incoming and outgoing accounts can be drawn up.
- Reintroduce, on an intermediary network layer, a “territorialisation” of facts and participating parties. The aim is to ensure that people and places can be guaranteed within the current communications system, whose weakness stems precisely from the difficulty in identifying and authenticating these parties, as well as actions in terms of time and place.

By partially moving system control towards establishing data either *a priori* or *a posteriori*, these two approaches are likely to considerably diminish or at least reduce the need for risky recourse to cumbersome identification methods through permanent and intrusive monitoring of all data flows.

In this light, the following should be examined, with particular attention to the issues created in highly distributed service-oriented architectures (e.g. cloud computing):

- An interoperable, accountability framework, including consistent interpretation of security policy agreements; implying the need for appropriate standards for protocols and interfaces, and for tools to enable compliant usage;
- Accountability balanced with privacy: investigation of protocols that can actually address both;
- Delegation, proxy, anonymity management;
- Non-repudiable processes/records;
- Context-dependent attributability;
- Channels for investigation, analysis, liability and redress;
- Real-time, large-scale test-beds for crisis management procedures;
- Domains of accountability to protect the interests of users;
- Close attention to the engineering and economics of accountability: raw audit-trail information generated has the potential to drown the system.

Closely related, are the business requirements for accounting, billing and charging for services or facilities. Accountability processes have traditionally been based on audit trails and attribution of actions. In addition we now require:

- Anonymous/pseudonymous charging and payment systems;
- Anonymisation or impersonation heuristics to produce untraceable, but trustworthy, valid sources/channels for information; for example, for economic, social or health-related statistics.

E-Identity

RISEPTIS recommendation 3 calls for the development of a common EU framework for identity and authentication. It is recognised that there will not be a single, unified format or scheme for eIDs, and that there will be multiple national or regional and commercial eID domains. There is also broad consensus on the need for flexible identity systems where users might have an *à la carte* choice (as an aspect of user-centricity) regarding identity-data options:

- The ability to decide on the level of security of their data streams (sent or received);
- The ability to decide the level of anonymity of these data streams:
 - The ability to choose from several possible connection types, according to the desired level of anonymity.

- At each of these various levels, only the aspect of identity required for that particular connection is revealed.

These options give rise to a number of challenges, which would expand the development of underlying mechanisms and techniques, and use what is already available. The following should be explored from a user-centric perspective:

framework to support interoperability between different schemes and environments (between, say, *mobile* and the *cloud*) with support for and use of partial IDs⁴

- functional requirements; e.g. as an enabler for access control and accountability;
- lifecycle management of eID, including protections to restrict loss, theft, error:
 - network level – accountability to balance privacy and traceability
 - service level – pseudo-anonymity
- framework to support interoperability between different schemes and partial IDs⁵
- linking IDs with dependent concepts, such as accountability
- claim-based approaches using novel and existing cryptographic protocols to eventually avoid architectures with a central component that everyone needs to trust
- (technology supporting new) business models for central, decentralised, and claim-based approaches;
- communication setup and routing that are identity-data-aware only as necessary for the functions of the network, without making the related users identifiable.

Privacy

Objectively verifiable data was previously compiled and managed for specific and acknowledged purposes. Now, however, data-gathering systems operate greedily and indiscriminately, grabbing data from each and every source. This opens up new possibilities for tracing, monitoring, shadowing and digital inquisition, with the possibility of registering and following every move of every object and processing and cross-referencing this data⁶. The technical paradigm shift goes from new identity management schemes and purely technical solutions to holistic societal approaches, since absolute anonymity may be neither possible nor applicable.

To protect the identity-related data of the user, the following should be examined:

- fine granularity access control to identity-related information;
- further development of Privacy Enhancing Technologies (PETs); tools to check privacy assurance and tools to advance transparency regarding used data;
- use of policy-based automated controls to manage the entire lifecycle of personal data in accordance with the dynamic needs of the data subject and the data users;
- methods for capturing detailed personal consents and preferences/requirements, representing these and rigorously managing their subsequent evolution, including revocation/retraction;
- possibility to retain control of personal data in environments with differing levels of trust from those to which it is initially disclosed, in accordance with associated policy mandates;

⁴ See D3.1a – *a la carte* identity

⁵ See D3.1a – *a la carte* identity

⁶ O'Hara, K., Tuffield, M. and Shadbolt, N. (2008) Lifelogging: Issues of Identity and Privacy with Memories for Life. In: Identity and the Information Society, 28-30 May, 2008, Arona, Italy.

- personal/communal collector of personal garbage/litter;
- use and control of identity-related information for network (e.g. routing) purposes without compromising privacy;
- standardised techniques to assure privacy across the various internet layers, through to network level and maintaining consistent privacy across different environments;
- tools and concepts for deleting data in the internet (“forgetting”).

Protection

Related to **Privacy** (including business confidentiality), the protection of data processing, storage and transmission, as well as the shielding of resources and assets (information, services, devices, communications) require the following:

- domains, partitioning, compartmentalisation – leading to trusted zones (and therefore, intermediate, semi-trusted zones), and to the localisation of damage;
- fine granularity access control based on multiple bases for authentication and authorisation. For example, IDs, privileges, roles, etc;
- mutual authentication, with multiple devices (ideally, technology invariant);
- new cryptographic techniques which are low cost but high performing, in preparation for the quantum/post-quantum age;
- uses of eID and its components in protecting the interests of its subject (data protection, etc.)

Usability

The Future Internet, and more generally, tomorrow’s communication networks, look to have one overriding feature: they will be focussed squarely on the individual (the citizen, the end user, the consumer). The aim of all future R&D programmes will be to influence the nature and scope of this central position. There are two viewpoints to consider:

- Does “being central” mean being observed (even monitored, spied upon) by the surrounding system? This would allow the automatic configuration of the surrounding system/services to suit the user’s tastes/requirements.
- Does “being central” mean that one’s choices will interact with and influence one’s environment? That is, do surrounding systems support voluntary disclosure of user information and can services subsequently be re-configured to reflect such disclosures?

There are trust issues in both these instances: Do users trust the first system enough to allow it to effectively spy on them? Do users trust the second system enough to disclose their data to it? The challenge here is not to offer users a stark choice between one or other of these two options, but rather to address the downside of both.

Making usability a permanent requirement of engineering would be a step in the right direction when addressing this challenge. Specific engineered-based research is therefore required to address the following issues:

- What does the user want or need by way of security and trust facilities and functionality? (including non-technical, human aspects) - how is this delivered?
- What are the impacts and implications for the underlying mechanisms and functionality?
- Attention to user/system interaction: sympathetic user interfaces, but with advanced options

- Tools and technologies to overcome users' limitations with respect to using and applying security, trust and privacy mechanisms; this may include decision support, recommended options, and the capturing of user preferences (profile).

Management and Governance

The proper management and operation of security policies must be considered in the context of the environment in which they operate. These settings could be ambient, heterogeneous, volatile, etc. Continuity of security relationships within these dynamic environments must also be appropriately managed (if unfeasible, what alternatives can be implemented under this guiding principle?). Control could be possible at all levels: self-controlled, user-controlled, centrally controlled or community controlled.

- A framework for consistent expression and interpretation of security policies, and the means of and implementing policy intentions at all levels, from network layers up to business and legal needs.
- Technical support must be provided for the high-level political decisions made in regard to sovereignty/legal frameworks across different jurisdictions. At a simpler level, the regulatory aspects to support the interoperability of security policies are necessary: from civil law for individuals and society, and contract law for business, to *common law* and the support of small claims.
- The relationships between eIDs and Government (.gov) must be given special attention – registrations, births, marriages, deaths, etc.

Socio-economic

RISEPTIS Recommendation 2 calls for convergence of technology with other areas and disciplines; Recommendations 3 to 6 contain specific requirements for parallel advances in non-technological areas.

- The role of other business/industry should be examined to learn how they handle security/risk-analysis. For example, can the insurance industry balance risk and cost for different categories of users? This could lead to the formal certification of trustworthy products/services and the classification of users. Using the insurance analogy: no-claims discount, additional premiums for risky use, exclusions, etc.
- Economics and inertia in the market place – why has security and trust been undervalued? – but possibly need to approach via the cost of insecurity; and user-perception of value of trust and security versus goodies and add-ons;
- The EU legal framework should be incorporated, including all jurisdictions currently covered, together with new laws and regulatory measures if necessary.
- There should be constant engineering vigilance about economic viability. Is it more cost-effective to prevent a data breach or just address the consequent damage when one occurs?
- The market place and related drivers for eID management (and other security and protection) should be explored:
 - To place Identifying credentials on different platforms;
 - Users can switch from one to another if not happy;
 - Economic value of secondary usages?

A1.2 Working Group findings (landmark topics)

Two related themes have led the thinking of the Working Groups:

- **user-centricity: placing the individual user at the centre of considerations and requirements**
 - rebalance relationship of user/consumer with service providers
 - control over *MY* identity/data
 - usability/accessibility of security facilities
 - protect users, (from others and themselves)
- **the need for the users to be able to trust their own digital environment as part of a larger ecosystem – the *network, Information Society* or even *cyber-space***

In this context, the following areas for further research were identified by the two Working Groups. For further details on these areas, please refer to the consolidated findings of the two Working Group workshops in Annex A.

Architecture

- Architectural issues, e.g. dynamicity, accountability, transparency, etc.
- Architecture for Trust and Security
- Interoperability

Instrumentation

- Measurability, Metrics, Transparency

Accountability

- Accountability and Responsibility
- Accountability

Trust engineering

- Trust Management & Governance
- Virtual social control, e.g., virtual neighbourhoods, including reputation systems

Identity

- Methodology for multi-party security and privacy IDM design, including metasytem standardisation
- Identities and Identity Management
- Non-declarative strong authentication

Privacy and data-protection

- Privacy transparency tool support
- “Minimum disclosure” credential management
- Privacy friendly biometrics– “One way” enrolment & usage protocols

Usability

- User support and orientation
- Use of Services
- UI design according to privacy requirements

Engineering & technology

- Technologies and Engineering to support multi-level security and assurance
- Virtualisation

A1.3 FIA (Future Internet Assembly)

The Future Internet Assembly (FIA) has held four events to date: Bled, Madrid, Prague and Stockholm. Breakout sessions and discussion on trust, identity and privacy have taken place at each meeting. These discussions have also informed the research and development challenges outlined in D3.1B.

One of the chief FIA goals is to identify cross-domain research themes, among the different cluster areas⁷, namely:

- Management and Service-aware Networking Architectures (MANA);
- Services and Software (platforms and infrastructures);
- Content Creation and Media Delivery
- Trust and Identity;
- Internet of Things;
- Real world Internet;
- Future Internet Research and Experimentation;
- Future Internet Socio-Economics.

More information on related cross-domain issues (including presentations, position papers and event reports) arising from the FIA sessions is available at the 'Trust and Identity' wiki⁸ (facilitated by Think-Trust) and the FIA page of the European Future Internet Portal⁹.

A2 Context

This section provides a background context (trends, threats, vulnerabilities and risks) for the trust and security research challenges identified in section 4 of this Deliverable. It also lists the landmark topics identified by the Think-Trust Working Groups, as well as briefly describing how the Future Internet Assembly events¹⁰ have informed the deliberations regarding the identification of future research challenges.

The overall challenge context continues to be the development of a *pervasive and trustworthy network and services infrastructure*, with the *Future Internet* as the bed-rock of the Information Society.

1. Trends

Some key features are noted here as drivers of future research action:

Increased, heterogeneous accessibility to converged information and services. (For example, ubiquitous, mobile access, very high bandwidth fixed networks and access);

Networks and future communication systems will have to move on from the concept of end-to-end connectivity (as in the current Internet) and embrace situations in which nodes are devices which cooperate freely and spontaneously in the absence of centralised services. Ubiquitous communication systems will demand new architectures based on the independent devices, connectivity reduced to

⁷ <http://www.future-internet.eu/home/clusters.html>

⁸ http://security.future-internet.eu/index.php/Main_Page

⁹ <http://www.future-internet.eu/home/future-internet-assembly.html>

¹⁰ <http://www.future-internet.eu/events.html>

fragments and spatial awareness of the nearby environment and local data through different nodes in the network.

Increasing volume of transactions, and even higher volume of traffic;

The advancement of digital technology in all areas is accelerating the rate of expansion in the volume of computer data and of the massive integration of software into our daily lives. Seamless digital technologies will gradually surround individuals, creating a tight mesh and a digital environment, which will profoundly increase usage. That is, the establishment and interoperation of the three complementary, ubiquitous environments:

- computing (information stored, processed and presented here and now),
- communication (access anytime, anywhere, using the best available channel) and,
- storage (collected, stored, described and displayed information and knowledge, available anywhere, anytime)

Large growth of sensors and slave-labour devices (*Internet of Things*), taking over the management of routine operations in commerce, utilities, the environment, and law enforcement and security provision;

We are seeing an emergence of contactless smart cards and radio-frequency recognition labels (parcel logistics, pet tagging, etc), networks of sensors in towns (multiple-window cameras), in the countryside (forest fire and earthquake detectors), in businesses (real-time warehouse inventory, mobile vehicle fleet sensors), networks in our homes and cars, personal assistance robots, tele-diagnostics etc. Whilst the current internet has connected 1.5 billion computers and mobile phones have connected 4 billion people, the Internet of Things may connect hundreds of billions of objects.

Increasing mobility of users (physical or virtual), seeking either continuous (mobile) or intermittent (nomadic) connection and access to information and services;

Nomadism¹¹ and/or mobility¹² destabilise the secure, personal cyberspace that is available when the user/device is static. The security of mobility requires an anchor of geography and time. Nomadism and mobility emphasise the need for a spatiotemporal security framework based on the *hic et nunc* (Latin for "here and now").

Convergence of types: voice, visual, entertainment, social and business services. (For example, twitter.gov, and 'official' blogs)

The widespread interconnection of networks and digital convergence further accentuates the computerisation process, which is making computing, telephone and audiovisual information increasingly compatible and interoperable. Progress in wireless technology has made possible the popularisation of mobile communication and has very substantially changed the way that businesses operate.

Nano to mega computing and communication – from (i) cheap, incoherent, tiny, low-resource entities in massive numbers handling the routine, to (ii) the gigantic cooperative high-resource super-grids addressing the difficult and complex

Computing will involve minuscule, sometimes invisible objects, with scarce resources, which are possibly non-identifiable but only traceable. These will be the end-points of a network which no longer has a few billion capillaries, but rather several Tera-nodes. Research on nano-architectures, nano-applications, and nanoprotocols, will transform the new network suburbs.

¹¹ *Intermittent connection and session from various locations*

¹² *Continuous connection to a digital infrastructure and activity on the move*

At the other end of the scale, computing will involve gigantic, complex poly-infrastructures (Internet, GRID, GSM, 3G, Galileo/GPS, the Internet of objects, Earth observation satellites). Computing of the gigantic means new services (Internet Telephony, Skype, etc.), which are also tools for surveillance, anticipation, crisis management, etc.

All of these have implications for the way society operates, and will make new and increasingly demanding requirements for trust from the users/consumers.

2. Existing threats, vulnerabilities, risks

The defects and failure/damage opportunities of the current Internet include:

- Fragility – networks and end-systems are vulnerable to simple attack, with information easily accessed, destroyed, copied and stolen, or falsified;
- Software is subject to design, implementation and usage errors, (hardware is not faultless, but more easily verified during design);
- Domino effect across inter-dependent systems in the case of accidental malfunction and/or failure, and attack propagation;
- Unprotected networked data exchange, but also via external media;
- Lack of user-awareness regarding their data, together with difficulties in understanding and availing of privacy-providing tools. The burden to the user in using these often complex tools hinders their acceptance and uptake;
- Basic usable security and trust facilities that enable the user to make informed choices or decisions.

Some malicious specifics:

- Fraud – breach of enterprise records/systems, stolen/captured credit card and bank details;
- Intrusion – Trojans: key-logging; colonisation, 'hacking';
- Impersonation through identification theft or failure;
- Phishing etc. relying on deception (spoofing) of user;
- Identity profiling from digital trails;
- Unauthorised disclosure: 'inside jobs' (police, government agencies, etc. for press and private investigators);
- Malware – viruses, worms, etc., for vandalism or blackmail/ransom threats
- IPR abuse – unauthorised file sharing, plagiarism;
- Denial-of-Service attacks

Unjustified trust – use of the 'open' net for sensitive operations (own goals):

- Defence-related – internet gateways to 'secure' systems;
- Emergency services;
- Utility management;
- Health systems;
- Financial/economic systems;

3. New threats, vulnerabilities, risks

New architectures will include structures and protocols that handle the blurring of boundaries between:

- what previously would be identifiable as domains (of, say, responsibility or control);
- real, logical, and virtual domains;
- where functionality actually lies – in hardware, in software, in the network, in information itself;
- what is an application and what is a service?

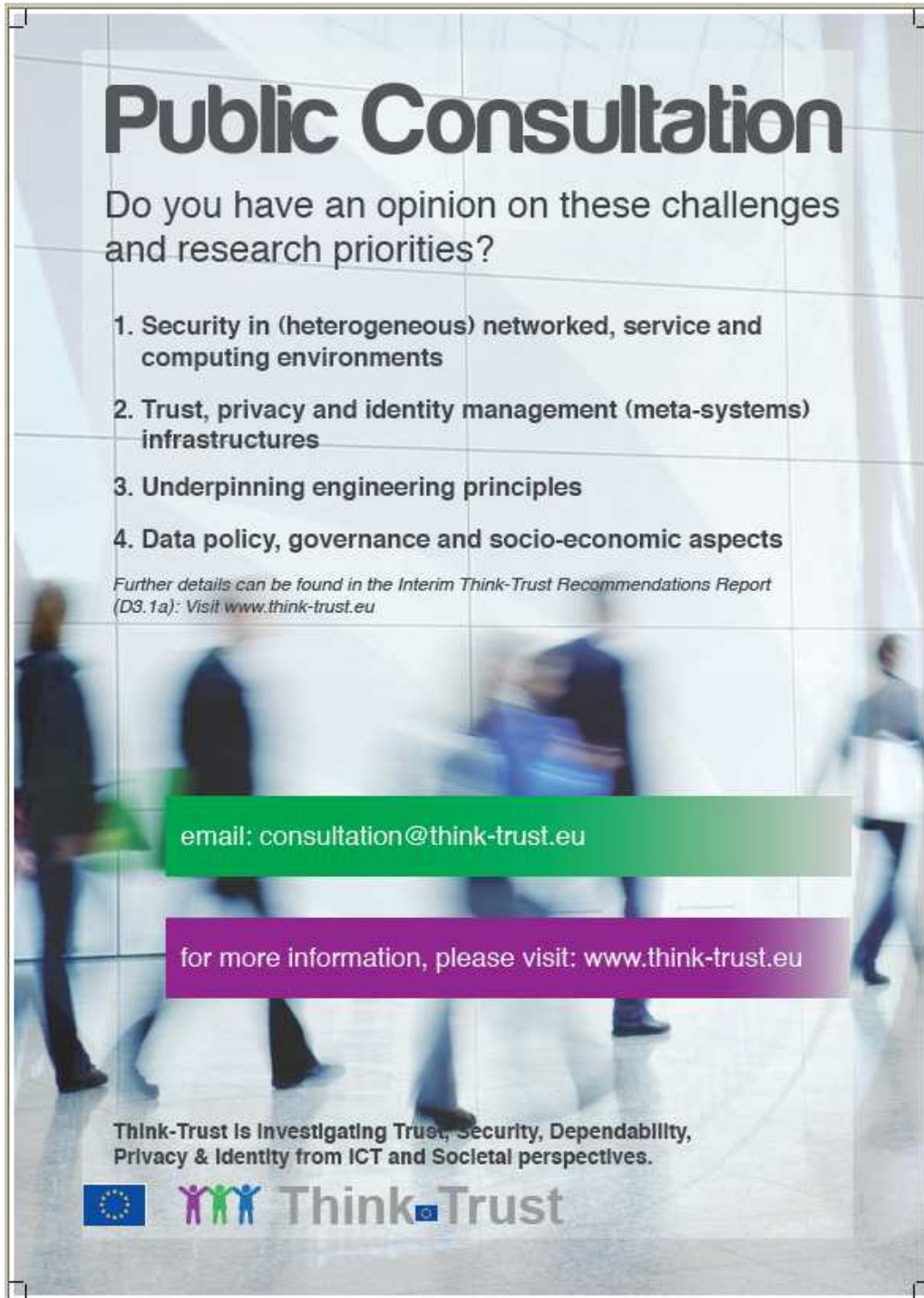
These all raise new, and extended security problems, not least from their volatility and fluidity. Attention is required to ensure that the new architecture (as a whole) pays attention to its *own* security needs and implications, as well as those of its *clients*.

Specific potential for vulnerabilities comes from the increasing integration of services. These include large and critical societal infrastructure, such as power and water distribution systems, transport communication means, and information and communication systems which support these infrastructures. This gives rise to the possibility of avalanching failure.

A consequence of this total penetration of our lives is the danger of the diminution and dilution of personal privacy and sovereignty (and that of enterprises or even administrations) – the possibility of multiple *big-brothers* watching, recording, and analysing our actions.

As new more comprehensive and complex trust and security measures are introduced, they bring with them new requirements for the non-expert user to be informed and to make appropriate decisions – in many cases, < I ACCEPT > the informed default advice from the “security” interface.

Annex B Public Consultation Poster



Public Consultation

Do you have an opinion on these challenges and research priorities?



1. Security in (heterogeneous) networked, service and computing environments
2. Trust, privacy and identity management (meta-systems) infrastructures
3. Underpinning engineering principles
4. Data policy, governance and socio-economic aspects

Further details can be found in the Interim Think-Trust Recommendations Report (D3.1a): Visit www.think-trust.eu

email: consultation@think-trust.eu

for more information, please visit: www.think-trust.eu

Think-Trust is Investigating Trust, Security, Dependability, Privacy & Identity from ICT and Societal perspectives.

  Think-Trust