Grant agreement number: 216890

Think-Trust
www.think-trust.eu

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

D3.1B Recommendations Report (Interim)

Start date of project:	1st January 2008
Duration:	30 months

Contents

1 Introduction

The RISEPTIS Advisory Board report '**Trust in the Information Society'**[1] sets out the high-level risks and challenges associated with trust in our digital environment (Cyberspace, Information Society, Future Internet, etc.). Trust is required to support our growing dependence on this digital environment for many aspects of our private and working lives. The report makes six recommendations for action in this respect.

The Think-Trust deliverable D3.1 is complementary to the RISEPTIS report, and should be read in the light of the RISEPTIS recommendations. The deliverable focuses on the research challenges which need to be addressed to realise the RISEPTIS recommendations. These challenges and research priorities are consolidated from the perspective of the Think-Trust Working Groups (WGs), which have met twice in plenary session since the start of the Think-Trust project. Deliverable D3.1 is an iterative document, refined in three versions;-

- D3.1A, produced in Summer 2009, outlined a broad vision of a digital future, its benefits and possibilities, and consequent risks and dangers.
- **D3.1B, highlights a set of interim research challenges, arising from the RISEPTIS Report. Further detailed background on aspects of these challenges can be found in D3.1A[2]. D3.1B is being submitted to the Commission as input to their deliberations on the 2010 Work Programme.**
- D3.1C, due for completion in Summer, 2010, will take account of input from various stakeholders and interest groups. A public, online consultation process[3], launched at an FIA workshop on October 7th, 2009, has been initiated to secure this input. The inputs will be used to refine and further develop the challenges identified D3.1B. The third and final version of D3.1 (i.e. D3.1C) will present the results of this public consultation process.

Figure 1 shows the development of D3.1, throughout the Think-Trust timeline:

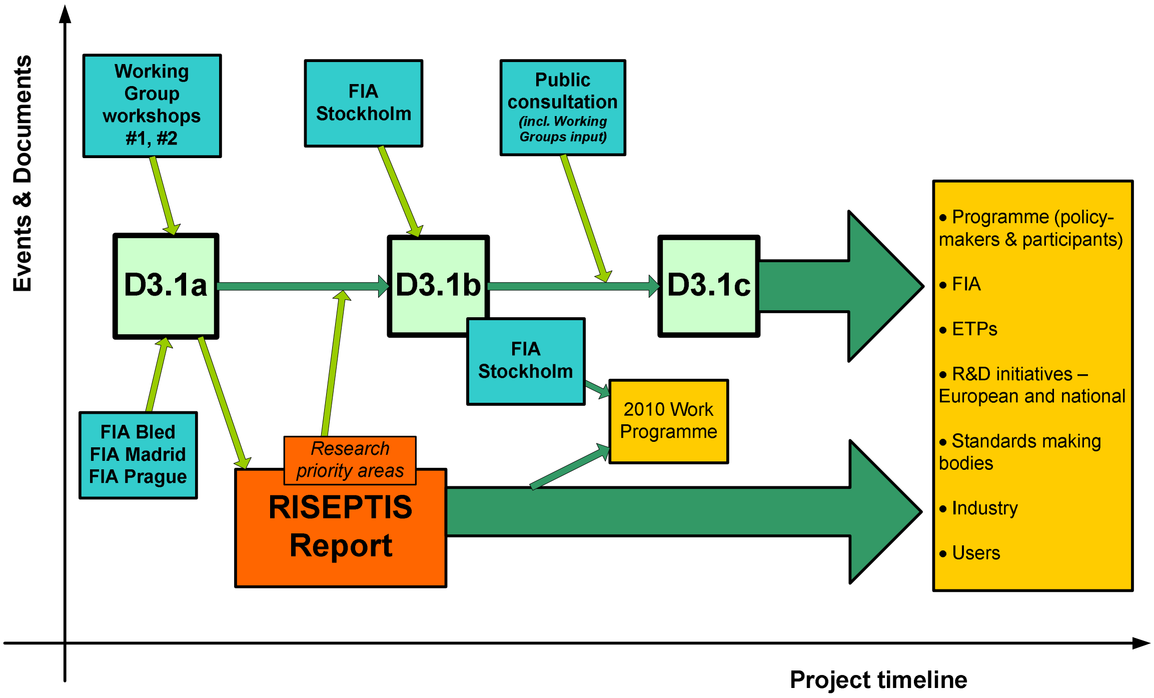

Figure 1 *Development of D3.1*

[1] http://www.think-trust.eu/riseptis.html

[2] http://www.think-trust.eu/downloads/public-documents/deliverabled3-1a/download.html

[3] http://www.think-trust.eu/general/news-events/public-consultation-launched.html

2 RISEPTIS

The RISEPTIS Report[4] identifies six high-level recommendations. The focus of deliverable D3.1B is to detail the research challenges arising, in particular, from recommendation 1 in the RISEPTIS Report, which recommends the stimulation of inter-disciplinary research in the area of trust and security.

Deliverable D3.1B also gives a high-level examination of the research and technology implications of the other five RISEPTIS recommendations. However, these require substantial social, legal, and regulatory developments, in addition to the development of appropriate technical infrastructures.

The six RISEPTIS recommendations are outlined below:

2.1 Research, technology development and deployment

Recommendation 1: *The EC should stimulate interdisciplinary research, technology development and deployment that addresses the trust and security needs in the* Information Society*.*

This recommendation is specifically about advancing European Research and Technology development. Four priority areas are proposed by RISEPTIS. These priority areas reflect the inputs that have been provided to the RISEPTIS Advisory Board by the Think-Trust Working Groups. The four priority areas are:

(a) Security in (heterogeneous) networked, service and computing environments, including a trustworthy Future Internet;

(b) Trust, Privacy and Identity management frameworks, including issues of meta-level standards and of security assurances compatible with IT interoperability;

(c) Engineering principles and architectures for trust, privacy, transparency and accountability, including metrics and enabling technologies (e.g. cryptography);

(d) Data and policy governance and related socio-economic aspects, including liability, compensation and multi-polarity in governance and its management.

These four areas are not independent and have many common underlying concepts and mutual dependencies, (which is reflected in our approach to the identification of the research challenges in section 4).

2.2 The interplay of technology, policy, law and socio-economics

Recommendation 2: *The EC should support concrete initiatives that bring together technology, policy, legal and social-economic actors for the development of a trustworthy Information Society.*

There is a need for a supportive, non-technological framework that should be developed alongside the technical elements. For example, there is a need to provide:

- Regulatory backing for accountability between Member State jurisdictions (or beyond), as is already the case for data-protection.
- A framework for common (or mutual/reciprocal) legal recognition of e-identities and the support aspects of interoperability, (noting past histories of, say, digital signature).

Research should not be confined to a one-way flow of regulation to support technical advances. However, it has proved difficult in the past to develop the contra-flow of ideas and the demands of those with a socio-economic perspective, where, apart from privacy and data-protection, we have often had to rely on technologists putting on their citizens' hats to articulate the needs of individuals and organisations.

In addition to the engineering aspects of trust, the non-technical social and psychological components must also be understood and put into context.

[4] http://www.think-trust.eu/riseptis.html

2.3 A common European framework for identity management

Recommendation 3: ***The EC, together with the Member States and industrial stakeholders, must give high priority to the development of a common EU framework for identity and authentication management that ensures compliance with the legal framework on personal data protection and privacy and allows for the full spectrum of activities from public administration or banking with strong authentication when required, through to simple web activities carried out in anonymity.***

This recommendation crystallises the two previous recommendations around a specific use case. The requirements of this spectrum must be explored. These include simultaneous demands for the rigorous protection of privacy, with equally robust attention given to identification and authentication of interacting entities, as well as the control, monitoring and accounting for subsequent operations.

In bringing forward the achievement of specific societal goals as part of an economic recovery programme, a large scale project has been proposed (RISEPTIS recommendation number 5) that would seek to unify and integrate various disjointed approaches to e-identity that currently operate in different European e-commerce and e-government service sectors. This initiative needs to take into account the requirements of a broader range of users (consumers) and providers of services. This will allow the appropriate engineering of solutions or the identification of further research areas.

2.4 Further development of EU legal Framework for data protection and privacy

Recommendation 4: ***The EC should work towards the further development of the EU data protection and privacy legal frameworks as part of an overall consistent ecosystem of law and technology that includes all other relevant frameworks, instruments and policies. It should do so in conjunction with research and technology developments.***

The main technological direction underpinning this recommendation is the support of legal and regulatory initiatives already under way to extend the vision of privacy and data-protection. Further research into technologies for protecting and minimising the propagation and disclosure of personal information is required to combat increasing risk of accidental or coincidental exposure.

The lapses in duty of care by data controllers will be more easily identified and attributed with the tracing and accountability capabilities recommended for inclusion in the underlying architecture.

2.5 Large scale innovation projects

Recommendation 5: ***The EC together with industrial and public stakeholders should develop large-scale actions towards building a trustworthy Information Society which make use of Europe's strengths in communication, research, legal structures and societal values - for example, a Cloud which complies with European law.***

Much of the basic technology to support further work towards trust in the information society is well known. However, certain incentives and stimuli should be applied to develop these technologies to overcome inertia and to mainstream their use. There has been a lack of long-term vision in the industry, both suppliers and consumers – 'where's the business case?' – allied with a head-in-the-sand attitude to the exposure and damage being sustained, not so much by e-business itself, but more by a commercial world that is under increasingly organised attack. Large-scale projects will provide a stimulus, putting some urgency into the supply-side and demonstrating benefits to the consumer/demand-side of business.

2.6 International cooperation

Recommendation 6: ***The EC should recognise that, in order to be effective, it should address the global dimension and foster engagement in international discussions, as a matter of urgency, to promote the development of open standards and federated frameworks for cooperation in developing the global Information Society.***[5]

[5] Work in this direction is already underway via the Coordination Action project INCO-TRUST (www.inco-trust.eu)

Europe cannot act in isolation. There are indeed many benefits that will accrue from establishing a solid European platform for trust, but given the inherent global nature of the Internet and the Web, Europe must collaborate with international partners to **establish standards that will enable trusted interoperability**. As well as the necessary technical standards, there must be corresponding standards on privacy and data-protection norms. These should not only regulate what happens to information within signed-up domains, but also regulate the behaviour and accountability of the data-controllers.

The development of new approaches, such as Cloud computing, increases the urgency for regulatory and technical standards. The essence is that services are ubiquitous and pervasive, which in turn contributes to their dependability and cost-effectiveness. To this must be added the other dimension of trustworthiness. The mirror image of this is of the globally mobile or nomadic user whose requirement is for a consistent, trusted service wherever and whenever.

3 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 events[6] 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.

3.1 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 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;

Nomadism[7] and/or mobility[8] 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).

[6] http://www.future-internet.eu/events.html

[7] *Intermittent connection and session from various locations*

[8] *Continuous connection to a digital infrastructure and activity on the move*

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.

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.

3.2 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;

3.3 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.

3.4 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 metasystem 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

3.5 Future Internet Assembly Events

The Future Internet Assembly (FIA) has held four events thus far, in 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 this interim Deliverable.

One of the chief FIA goals is to identify cross-domain research themes, among the different cluster areas[9], 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;

[9] http://www.future-internet.eu/home/clusters.html

- 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' wiki[10] (facilitated by Think-Trust) and the FIA page of the European Future Internet Portal[11].

[10] http://security.future-internet.eu/index.php/Main_Page

[11] http://www.future-internet.eu/home/future-internet-assembly.html

4 Research & Development Challenges

This section outlines the key research challenges that require attention in order to provide trustworthy hardware and software for the Information Society, based on the four priority areas identified by recommendation 1 of the RISEPTIS Report. The research challenges also take account of the context set out in section 3 of this document (Working Group findings, FIA outputs, etc.), as well as recognising the topics already covered in previous calls (up to Call 5).

4.1 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.

4.1.1 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?

4.2 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.

4.3 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 CERT[12] teams and ENISA[13] would be of added benefit to this goal.)

4.4 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:

- 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

[12] http://www.cert.org

[13] http://www.enisa.europa.eu

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.

4.5 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 IDs[14]
- functional requirements; e.g. as an enabler for access control and accountability;

[14] See D3.1a – *a la carte* identity

- 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 IDs[15]
- 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.

4.6 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[16]. 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;
- 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“).

4.7 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:

[15] See D3.1a – *a la carte* identity

[16] 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.

- 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.)

4.8 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).

4.9 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.

4.10 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?

Annex A – Working Group Workshops: Consolidated Findings

Architecture

Architectural issues

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

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

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

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.

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 failure or non-compliance. The arena for all this is again the generalised, mobile, polymorphic dynamic environment. The big challenge is to achieve this goal without incurring burdensome operational overhead.

It appears that this particular interoperability requirement may have characteristics that are common to, or ‘typical’ of a number of basic functions that 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.?)

Instrumentation

Measurability, Metrics, Transparency

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

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

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

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

Accountability

Accountability and Responsibility

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

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

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

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

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.

Trust engineering

Trust Management & Governance

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

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

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

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

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

Identity

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

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

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

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 associated with 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.

Non-declarative strong authentication

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

Privacy and data-protection

Privacy transparency tool support

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

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

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

“Minimum disclosure” credential management

Although theoretical approaches and some prototyping do exist, we are still far from deployment in practice through lack of common UI design and policy standards (See points 3.1.6and 3.1.7, above).

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

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

Privacy friendly biometrics– “One way” enrolment & usage protocols

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

Usability

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.

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.

UI design according to privacy requirements

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

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

Interoperability and consistency of privacy policies calls for tools and standards.

Engineering and technology

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.

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.