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

D3.1a Recommendations Report (interim), including Annexes on WGs

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

Organisation name of lead contractor for this deliverable

Ecole Nationale Supérieure des Télécommunications (Télécom ParisTech)

Editor

Michel Riguidel
michel.riguidel@telecom-paristech.fr

Contents

Introduction and Background

The **Think-Trust** project is a Coordination Action whose main aim is to bring together the European R&D community in the field of Trust, Security and Dependability (TSD) and other important non-technical stakeholders that have an interest in the area and can contribute in a meaningful way, in the development of present and future programmes of Research and Development for ICT for Trust, Security and Dependability.

The approach taken in the Co-ordination Action is:

1. To consult with the users themselves, with those responsible for facilities and services, and with the researchers and developers providing the technologies, through a sequence of well targeted workshops with preparatory contribution and comment via our web-site; this stage will agree an outline framework that allows common understanding of requirements and of possibilities for solutions;
2. To set up a ***Think-Tank*** (RISEPTIS Advisory Board) of experts and representative voices to analyse and review the requirements and potential responses, which will ultimately lead to initial recommendations and options;
3. Take these back to the constituencies through workshops and web-based consultation process;
4. Compile final recommendations for future European R&D and for preparatory actions in other areas critical to long-term acceptance and satisfaction in the Information Society.

This Deliverable sets out the interim findings of the project concerning the main challenges and key research priorities in the area of Trust Security and Dependability. Section 1 of the document sets out the main issues relating to Security and Trust in the Future Internet: Section 2 sets out the main Security and Trust Challenges and Section 3 identifies four key research priorities :-

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 focuses on detailing the TSD research agenda which has been outlined in the report currently being drafted by the RISEPTIS Advisory Board. The Deliverable elaborates in more detail the four areas above, which will be identified in that report. This is an interim recommendations report and will be further refined and developed during the remainder of the Think-Trust project.

This interim report 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. An outline of accompanying measures in non-technological areas is also given. The final version of this report will provide specific recommendations and priorities for future work.

1. Security and Trust Context of the Future Internet

This section provides background information on a broad range of key issues that need to be considered when discussing Security and Trust in the Future Internet, providing a context for the challenges and research priorities in sections 2 and 3.

1.1 Ubiquity of the digital kingdom

1.1.1 IT evolution: Moore law, interconnection and usages' appropriation.

Progress in microprocessor technology, new paradigms in communication technology and the emergence of groups of networked sensor-actuators enable a vision of a new age for information processing in daily tasks.

The values of modern civilization are inevitably moving towards a more immaterial virtual world. Continuous electronic miniaturization, the acceleration of communication networks' performance and the inexorable deployment of computing infrastructures is creating a digital urbanization where everything appears closely connected, facilitating inter-communication and access to services and information. The imperial conquest 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. This computerization process is further accentuated by the widespread interconnection of networks and by digital convergence, 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. Seamless digital technologies, i.e. the establishment and interoperation of the three complementary ubiquitous environments of computing (information stored, processed and presented here and now), communication (access anytime, anywhere, using the available best channel) and storage (collected, stored, described and displayed information and knowledge, available anywhere, anytime) will gradually surround individuals, creating a tight mesh and a digital built-environment, changing usage and having a profound impact on civilization's values. The value of digital possessions may soon exceed that of material ones, for individuals, businesses and state institutions.

Future services will be based on the notion of context and on knowledge. They will have to cope with highly dynamic environments and changing resources, and will have to evolve towards more implicit and more proactive interaction with humans. Content providers will play a decisive role in this context.

Furthermore, networks and future communication systems will have to move on from the obsolete 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 centralized 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.

The concept of end-to-end is not in itself, obsolete. As long as single, point –to-point communications exist (unicasting), so will end-to-end. Unicasting would even seem to be the favoured mode of communication, both in the Internet and social sense. What is new, and constitutes the added value of the digital environment, are the new cooperating devices (instead of a centralized service) and the procedures for the establishment of these end-to-end connections.

1.1.2 The two frontiers: infinitely small (tiny objects) and large (complexity).

IT research must today address the two opposite aspects of the new boundaries of the immaterial world:

- Computing of the derisory: minuscule, sometimes invisible objects, with rare resources (in Watts, Mips, Bytes, Bits per Hertz and per second), possibly non-identifiable but only traceable , will be the terminations of a network with no longer a few billion capillaries, but rather several Tera nodes. Research on nano-architectures, nano-applications, and nano-protocols, will transform the new network suburbs. Undoubtedly, end-to-end will no longer

mean anything, and traditional protocols - IPv4 (and even less IPv6 !) will not withstand such brutal economies in computing and communication resources. New computing models will become necessary. We will have to segment models for computing, storage, and communication, which will only be applicable within a certain technological niche. Computing is not fractal!

- Computing of the gigantic and inextricable: poly-infrastructures (Internet, GRID, GSM, 3G, Galileo/GPS, the Internet of objects, Earth observation satellites) will be the new worldwide constructions of the (Violent) Virtual Village: interconnected, compatible, yet gigantic, inextricable, barely controllable and extraordinarily fragile. Computing of the gigantic means new services (Internet Telephony, Skype, etc.), which are also tools for surveillance, anticipation, crisis management etc.

1.1.3 Two structuring paradigms: virtualisation for the global and embodiment for the local.

In practice, these two opposite aspects complement each other and result in a duality, since the infinitely small strengthens gigantism, and vice versa. The mass of connected manufactured items that surround us will result in an environment characterized by excess. These extremes are addressed by two fertile, yet opposite, computing notions: virtualization and embodiment.

1.1.3.1 Virtualisation.

Virtualization is a powerful technique that has developed from its early use in large CPUs in the 1960s. It enables the construction and operation of composite *virtual* computing entities with desired properties and functionality from available *real* or possibly other virtual entities. It involves juggling with computing entities of various orders to create other, more effective, computing entities, by reducing the complexity of a system whose handling has been changed by applications and services. Just as the object approach has changed the way software is manufactured, the virtualization approach has transformed the treatment of computing architectures. Virtual memory has changed the writing of memory hungry applications; the Java machine has made it possible to encapsulate computer programs in HTML web pages, which has determined its success. Virtual private networks have generated digital trenches in public networks, which has created a certain privacy in a global no man's land and allowed companies to operate over the Internet. VLAN technology has made it possible to dissociate the logical LAN infrastructure from the corporate network and the physical infrastructure, which has largely contributed to the success of these networks. Virtualization enables the frontiers between two hardwares, or between a hardware and a software, to be abolished, the forms and standards between two databases to be erased, domains that differ in terms of management policy to be crossed, packets to be routed differently, and borders between technologies and heterogeneous networks to be crossed. Above John von Neumann's hardware and software subdivision, a virtual plain is in the process of settling permanently throughout computing architectures. All overlay structures, all superposition networks are also paradigms derived from this virtualization operation.

1.1.3.2 Embodiment, adaptation to the immediate environment

Embodiment is a notion contrary to virtualization that remains little used. While virtualization aims to annihilate figures that are rebellious to transparency and to a seamless world, embodiment makes it possible to design and reveal dynamic forms and, at the same time, creating intelligence locally, where there was none. Artificial intelligence and robotics are renewing themselves. While they proclaimed premature success in the 1980s, a new effective and pragmatic school is emerging with the fundamental notion that knowledge is not a result of information or computing. Intelligence is not only about computing, it demands a body (in the physical sense). The first successes are in the field of robotics recognizing their surroundings, understanding situations, and assisting individuals in everyday tasks. It goes without saying that this powerful concept will have considerable applications in the distributed world of sensor networks, of middleware, in security to supervise scattered situations and in computing in general.

While nowadays we have distributed systems and embedded systems, in the future we will supplement this range with overlaid systems (corresponding to virtualization) and embodied systems (corresponding to embodiment).

1.2 The three periods of a digital roadmap

1.2.1 The architecture- and format-cleaning period

This decade, digital technology has experienced a setback, namely, digital convergence, i.e. an ad hoc re-allotment of both architectures and formats. This attempt at realignment has consisted of cleaning up, retouching computers, televisions and telephones to make them interconnectable and interoperable. Digital technology has little connection with physical reality: few sensor networks, few robots (only 1 million in existence in 2008). Information technology is still operating behind closed doors. However, even a web in tatters, these interconnecting networks will conquer other territories and could absorb the telephony, 3G and television infrastructure. In its original, pioneering form, the web was an electronic whiteboard (the term web in fact comes from the acronym Wide Electronic Board), which became fragmented into pages scattered across different sites during the 1990s, which search engines attempted to classify and then recover; it is now in the process of transforming itself into a series of dynamic sheets of personalised information, virtually attached to every nomadic citizen. Thus the torn fabric of the internet is already showing its seams, stitches and hems: the search engines pick up these stitches, patches and hems which connect web-pages with links, peer-to-peer file download applications link processors and discs of adjoining computers in clusters to calculate and exchange in an evenly-distributed manner.

1.2.2 The ebullient period of reconciling virtual and physical realities

This retrenchment should change as the system evolves towards a reconciliation phase in which the virtual and physical, links between technology and reality, are reconciled. 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, telediagnostics etc. Whilst the current internet has connected 500 million computers and mobile phones have connected 2 billion people, the Internet of Things should connect 1000 billion objects. Malfunctions and attacks on these networks could cause widespread chaos.

With globalisation, China's increasing openness and new actors emerging onto the international scene, digital networks (which are a geostrategic challenge) are in danger of being structured around language and culture, exposing new models, counter-models and alternative models, whilst avoiding the providential solution of a model which is both unique and pseudo-universal. The future cyberspace is in danger of being structured around navigation and positioning infrastructures (GPS in the US, Galileo in Europe, Glonass in Russia, Beidou in China). The natural fragmentation around these new continental plates will create a digital tectonic which is likely to see the pull of regional standards drawing a new set of decentralised networks.

1.2.3 What lies beyond the horizon: IT at atomic level

In the future a new digital era of Nano, Bio, Info and Cogno (NBIC) will dawn, in which humanity will be working at atomic level (nanotechnology), with living tissue (bio-geno-technology) and photons (quantum computers). This will radically change civilisation. Bits of information technology will be able to pass between the cells and atoms of living beings in order to manage and control this invisible world. A completely new level of vulnerability and threat could arise from this nanoworld: Nano warfare, the trading of living cells, quantum warfare for breaking State secret codes; in short, a new confrontation at atomic level.

1.2.4 21st century science and information technology

Those countries that wish to remain in a pre-eminent position will have to learn to master Angström (10^{-10} m) technology at atomic level, and attometer technology (10^{-18} m) at quark level. Having taken on board the Einstein-Minkowski space-time theories, humanity should now be able to move beyond our 4-dimensional view, and begin to accept theories of a universe which comprises more than 4 dimensions (some of which are nanoscopic), and more than 4 forces. T Kalusa's first theories date from 1921! They remained in obscurity for over 50 years. String theory, branes and supersymmetries should come into their own within the next twenty years.

Information technology will become an integral part of everyday life, running through the very veins of reality and nature, creating a new thinking machine on a planetary scale, a new realm, alongside the animal, mineral and vegetable kingdoms. The new information technology of the 21st century will organise this invisible artificial world, this vast ubiquitous world. It will be a world away from the current internet, with its primitive architecture and which is so wasteful of energy and fuels the digital divide.

1.3 The fragility of the digital world

1.3.1 Threats and vulnerabilities

Despite the unquestionable success of digital technology, the resulting information systems are vulnerable because it is in the nature of their construction that the digital content is independent of its physical support. The digital environment is thus volatile: it can easily be duplicated or destroyed, stolen or falsified. Furthermore, since digital documents are read and written with equipment that uses software, and software nearly always contains errors or bugs, the possibility of some kind of malfunction is ever present.

In this way as society becomes increasingly dependent on digital technology, the environment provided by the technology becomes increasingly fragile. A major risk is inherent because our daily environment is determined by these complex systems that can break down or be paralyzed by malicious action, accident or failure. Since these systems are interconnected and interdependent they are exposed to domino effects that can quickly spread malfunctions in the operation of each system. Our attachment to these tools, which in the case of the Internet and mobile phones sometimes approaches addiction, does not help this situation of dependence on digital structures.

Lastly, let us not forget that the future of ICT raises human and social issues. What type of digital systems should we consider for daily lives that are compatible with our values; how should we view the relationship between knowledge and the capacity of physical persons and their cultural and emotional requirements? What are, what will be and what should be the social implications of the development, deployment and use of such systems? The evaluation of technology on a precautionary basis should guide the design of tools for the construction of ICT, ultimately not purely driven by the evolution of technology, but with a basic objective of improving the quality of life.

1.3.2 Is the Web about to unravel? The Internet is broken

Over the last few years, the very fabric of the internet has started to come apart, distended by new usages, pulled in opposing directions by successive hordes of new arrivals and defaced by the cyber-delinquents who exploit the web's pseudo-anonymity with impunity. The Internet, the network of networks, was never designed to be used on such a vast scale. Its size has been grossly overextended by the power of its services and the performance of its high-speed connections, which are inundated with increasingly voluminous content. 1.4 billion Internet users generate a monthly traffic volume of 10 exabits, requiring connections which can download 100 gigabits per second, to run such popular applications such as Skype, eBay, YouTube, Facebook, Amazon, BitTorrent, SecondLife, etc. The strength of the internet lies in its ability to have stood up to this new context, but its weakness is that is that it is unable to change its fundamental nature.

The hard-line internet extremists continue to trot out the dogma of network simplicity and performance, intelligence at both ends, free usage, transparent architecture and protocols and ease of connection. These properties have diminished over time such that we now see false simplicity with patches and spot repairs, inflexibility and over-sizing to absorb the multimedia

tsunami, complexity within the core of the network, a false idea of free access as, for example, someone has to fund investment in such innovations as fibre-optics etc., software obscurity, aggressive usage of standard protocols, the inability to manage mobility, partiality of governance, security lapses through identity fraud, a disregard for personal data protection, following insidious surveillance or even digital inquisition. The old internet model has coped with all of this.

The current Internet was unable to adapt either to mobility, or to modern security. The Future Internet (FI) will be polymorphous, created on the basis of different infrastructures. Therefore, it is necessary to incorporate into the Future Internet the split, the dynamic and evolving nature of digital systems and a strong holistic security design.

Our current information technology paradigms are in the process of being dissolved. The dichotomies between computer and networks, between hardware and software, between applications and services, between the logical and the virtual, between software and information, are in the process of being blurred or, more precisely, the terms of the division are radically changing meaning. Consequently, the security paradigms need to progress at the same rhythms as IT evolution.

1.4 Sovereignty and dignity (individuals, groups, states)

The values of modern civilization are inevitably moving towards an immaterial world. Continuous electronic miniaturization, the acceleration of the performance of communication networks and the inexorable deployment of computing infrastructures is creating a digital urbanization which facilitates communication and access to information.

Gaining control of information and its transport, enforcing the protection of owners' intellectual property, protecting teenagers against illicit acts and ensuring the security of stored, processed or conveyed data are becoming the major challenges of our countries in Europe. Protection of sensitive digital commodities (in the form of data, documents or other creative work) belonging to responsible entities (their authors or owner organizations) represents the new challenge of the administrators of the networks being woven and deployed all around us. The freedom of individuals, the survival of companies and the future of countries in all the fields of endeavour, whether in private or public life, in the civilian world or in the defence establishment need to be considered.

The digitization of the developed world is in progress, and the digital universe is intruding into all sectors of activity: industry, trade, finance, defence, administration, health, education, justice and environment as well as personal and social. The stakes of information security at the dawn of the 3rd millennium raise questions of sovereignty such as ownership of transport and storage of information over national territory, economic questions such as costing of on-line distribution of contents, sociological questions such as establishing citizens' trust in digital structures (the Internet, but also mobile telephony, banking or logistic digital labelling networks), as well as ethical questions such as recording, without their knowledge, the computerized data of people.

Digital personal data, which are recorded without the subject's knowledge, are for example, successive bank account transactions, geographical position within a telephone relay cell at the telecom operator, connections on the Web servers at te Internet access provider, appearance and behaviour on the cameras installed on public highways, the radio label (RFID) on clothing.

The security of the digital world has become a fundamental stake for the citizen with respect to individual freedom and protection of computerized identity and privacy, for the company with respect to the protection of its computerized industrial assets, the security of its business transactions and the trust level of its information networks, and for the state with respect to the reliability of operations and the reduction in the vulnerability of large and critical infrastructures : power and water distribution systems, transport communication methods and means, and information and communication systems pertaining to these infrastructures.

1.4.1 Sovereignty: Geo-Strategic Aspects

Digital security has assumed major importance in the civilian and business environment over the last decade. Security is closely related to geo-strategic, as well as to political, economic and social issues. Indeed, entire facets of daily life, of the economy and of administration are highly dependent

on information technology: transportation (management of the railway and air traffic), communications (telephony and Internet), the stock exchange, the trade system, the banking system, the health system (the social security smart card, the computerized medical records) and the defence system are examples of sectors relying on about a hundred computer servers. Rendering these servers secure is of critical importance as an attack against these computerized fortresses may result in the disclosure of vital information to the attacker or may paralyze an entire country or region.

It is therefore crucial for users, companies and the state to preserve their dignity, liberty and sovereignty, yet these rely on the control of the digital systems they use and the security of their operations and related information security.

1.4.2 Revaluation of the Digital Asset Base: The Economic Aspect

Individual, corporate and government assets are increasingly taking a dematerialized form, as the storage of digital data is becoming equivalent to productivity gains in all respects. The volume of data doubles each year and the value of family, company and government assets is increasingly derived from or encapsulated in this digital, cultural and industrial asset base. This is true for some new economy companies, whose industrial assets are already almost exclusively in intangible form (databases, computing programs, manufacturing secrets), overtaking in importance the buildings and possibly even the personnel administering it. However, this phenomenon will become a reality for the individual users as well. Archiving, restoration and search of personal databases, rerunning older software, replay of data, will become current practice among our countrymen. The government should take into account this essential aspect of the lifecycle of data from their creation through obsolescence and destruction, via utilization and reconstruction. The birth of the concept of digital assets represents a genuine rift that has much wider implications than information management in general: it includes management of Intellectual Property Rights (IPR), Digital Rights Management (DRM), copyrights and online sharing of information.

The security objectives related to the digital assets base are expressed in terms of confidentiality (non-disclosure to unauthorized persons), integrity (non-alternation of content by hackers) and availability (the ability of authorised users to access and use these assets without being hindered by unintentional or malicious acts).

1.4.3 Building and Maintaining Trust in Digital Infrastructures: A Sociological Issue

Large digital infrastructures are set in place all around us: mobile telephony, communication satellites, computerized banking networks, the emergence of digital television, smart tag logistic systems (RFID). Some personal digital objects have become irreplaceable (credit cards, mobile telephones) or sometimes indispensable (portable computers) or convenient to use (PDA's, digital cameras).

All citizens should embrace this digital world, without, however, abandoning the dropouts by the roadside (the social rift here is rather of a digital nature). Due to its highly complex and diverse nature and to its rapid development, the digital world can no longer be mastered: computer science has accustomed us to bugs, while software or products that work poorly if at all are hardly a rare occurrence. All these reinforce the sense of mystery in the minds of laymen.

Information security is related to the level of trust. If we wish all citizens to share these conveniences and adopt the new technologies, we must establish and/or restore the trust of individuals, companies and government. To this end, the concept of "digital governance" exercised by the international community has become necessary, as the digital world can no longer be left to the will of market forces.

1.4.4 The duality between digital privacy and collective security: digital dignity

This illustrates the subtle relationship between the methods designed to preserve our privacy and the legal procedures to ensure it, and the practices intended to protect the rest of the world against our potential malicious or accidental actions, and the means that are being implemented to confine

them. Creating a climate of mutual respect and trust is not contradictory to devising and setting up mutual defence procedures.

Open and transparent dialogue should make it possible to negotiate the rules and subscribe to clear and harmonious security policies. Such digital dignity is achievable and required to preserve the democratic values of our civilization.

1.4.5 Confidence in the security offered: digital sovereignty

It is crucial that the security operating rules are open, transparent and well understood by everybody without the presence of hidden solutions of which people are unaware and that are out of their control. We must be offered tangible security that is verifiable or verified and certified by a trusted (state) authority in order to get confidence in the host of security tools we are offered. It is therefore important to insist on the guarantee, the certification, or the qualification ensured by a trusted entity and its experts. If, for example, security is designed in the dark and concealed in a black box, it will be impossible not only to analyze any residual weaknesses and vulnerabilities, and therefore to trust the system, but also to intervene in the event of an attack. Security specifications implemented could not therefore be an absolute industrial secret[1]. Moreover, (security) service providers should not establish a dominant power play between themselves and their users that would cause the latter to become sorts of "trusting slaves". For example, a trusted third party accepted by both could appreciate the technical measures and validate the actual levels of security implemented.

Today, ICT has reached a planetary dimension and is used by a broad section of public that handles and processes myriads of potentially vulnerable data. Security should then be perceived as a state of vigilance that ought to be implemented through a set of actions that is very well thought through: we need to anticipate problems and solutions rather than considering attacks like an unavoidable phenomenon of modern times and healing, at the end of the chain, the damages caused by cyber-crime. This is the challenge that we must face in order to gain the trust of citizens and companies and encourage them to use these technologies in a fruitful manner.

1.5 Creating a user-centred system

1.5.1 Focussing activity on three issues: who, where and when?

To specialist observers, the Future Internet, and more generally, tomorrow's communication networks (for we cannot discount the **coexistence of different forms and methods of communication**), look to have one overriding feature: it will be focussed squarely on the individual (the citizen, the end user, the consumer). This vision is, at this stage, neither optimistic nor pessimistic, as the aim of all future R&D programmes will be to influence the nature and scope of this central position:

- Will the individual passively occupy this central position, a mere consumer at the hub of immaterial radii? Or indeed,
- Will individuals be active in the sense that they can construct their own relationships, using an array of technical, functional and societal tools and specifications?

Put another way, this issue touches on our freedoms:

- Does "being central" mean being observed (even monitored, spied upon) by the surrounding system?
- Or does "being central" mean, conversely, that one's choices will interact with and influence one's environment?

So the issue is twofold: what rules will govern relations between future systems and individuals, and who will write these rules?

[1] Kerckhoffs' principle: a system should be secure even if everything about the system, except the keys, is public knowledge (Shannon: *The enemy knows the system*)

It is not enough however to maintain the primacy of the individual if we then ignore a parallel trend which both weakens and puts into a different perspective the aforementioned vision: the centre will potentially be everywhere, for everyone:

- The ubiquity of information technology and the supply to its access points;
- The dissemination of information (both spatially and thematically);
- The capacity to join spatially disparate sources of computing power;
- The rapid expansion of potential locations from which individuals can assert their presence via actions conducted over the network (relayed communication, remote function operation, etc).

The unity of a situation is often defined in the same way as the three theatrical criteria: unity of time, place and action (or person). How are we to ensure that these unifying factors continue to prevail in the future, if time (through programming activity) and place (through the multiplication of remote access points) are no longer reliable indicators?

It is incumbent upon future research programmes to restore spatial and temporal system guarantees (the where and the when, with sufficient certainty to ensure continued confidence), if we are to avoid seeing it diverge from this.

1.5.2 The postal model

What we shall call the **postal model** would be interesting to apply in at least five of its aspects:

- The Postal Service is a trustworthy infrastructure.
- The possibility of senders being able to transmit messages anonymously (unless they actually give their details on the back of the envelope).
- The impossibility of maintaining anonymity in postal services frequently used for official purposes, such as recorded delivery.
- Guaranteed dispatch point, thanks to the postmark (this does not indicate the sender's final destination).
- Date guarantee; this has a recognised value, since the postmark "authenticates" it (the postmark does not necessarily match that on the letterhead, nor the date on which it was placed in the post-box, as there may be a day or two's disparity).

Based on this postal model, it might be possible to draw up a set of technical specifications which could lead to concrete security policies and technical solutions for electronic exchanges.

With regard to the aforementioned third criterion of unity through action and person, it is worth highlighting the importance of the issue of identity: how can any person or object be reliably defined whilst respecting the need for relative anonymity or privacy as well as transparency? More prosaically, how do we avoid identity fraud or theft?

What we shall refer to as "unity of person" should be preserved by both legislative and technological means.

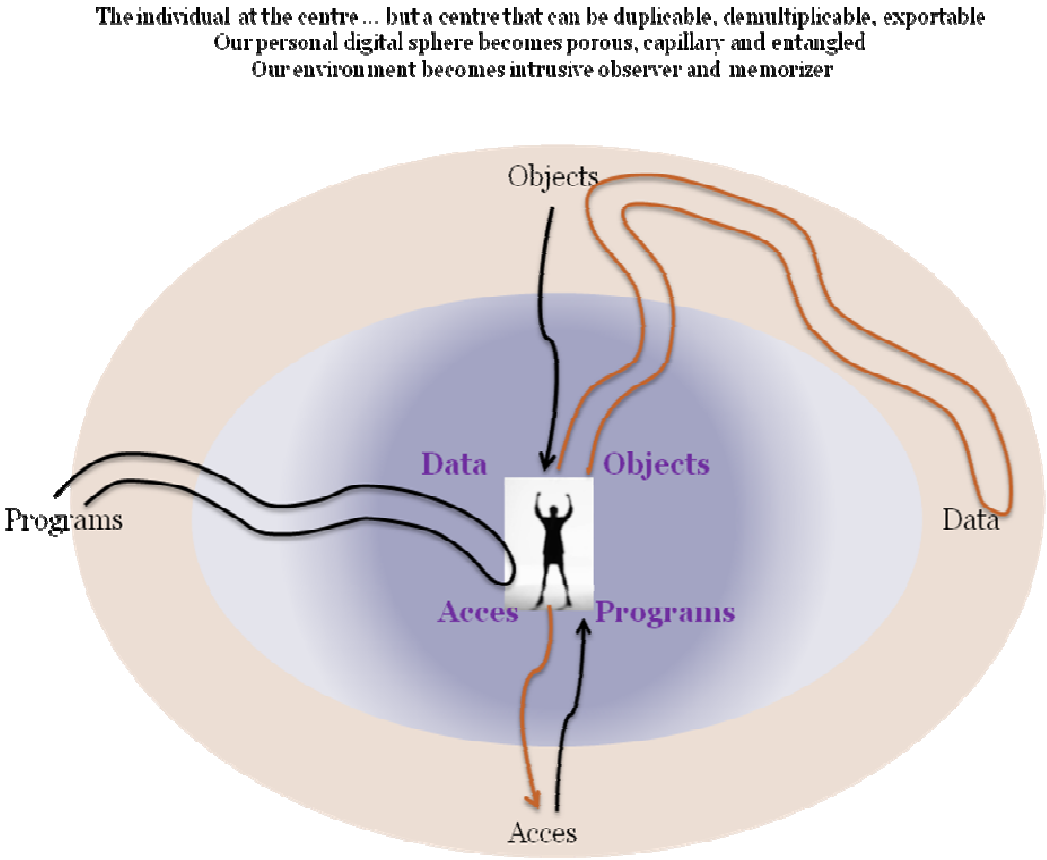

Figure 1: The individual will become the centre, but the centre will become duplicable, multipliable, remote-capable. Our own personal digital domain will become porous, capillary and disordered. Our technological environment will become one of intrusion, surveillance and record-keeping.

1.6 Security issues for business and society

The internet is a public space in which the security of infrastructure security for operators, and the security of software and data security is, for both their authorised users and owners, a guarantee of reliability. Despite the architectures deployed to ensure greater reliability and service connectivity and despite the anti-piracy measures taken to protect sensitive data, it is clear that computer systems regularly fail or are subject to malicious attacks.

Architectural security (future internet) and data security (software and data) represent key challenges. The digital world is one which is open to all: on the web, everyone is technically more or less free to post and to upload content, publish whatever they want online, write what they want to whomever they want; essentially to do whatever they please on the system which they choose or stumble blindly upon. The first phenomenon which everyone has experienced is the receipt of viruses via various entry/exit methods (networks, USB keys, CD-ROMs, etc), on the back of which the antivirus software market has experienced tremendous success, not necessarily justifiably, and the invasion of spam messages against which operators offer a filter to weed out this proliferation of inappropriate advertisements, which ultimately performs rather poorly.

Then there are more pernicious phenomena such as fraudulent and criminal acts which can be conducted over the networks. These include such acts as the theft of credit card details and sexual offences as well as sensational fraud and the propagations of ideas which call in to question the whole notion of democracy and respect for others. One of the challenges in guaranteeing a democratic world (as the internet does not recognise national boundaries), is to put in place a rigorous system of regulation on the one hand and effective policing of the network on the other. It would also seem to be imperative that the means of combating cyber-fraud be dealt with at national level, and that regulations governing business (access providers, software publishers, and hosting

companies) and the State be drawn up to ensure there is adequate legislation covering the issues of cyber-fraud and consumer protection.

1.7 Privacy issues for citizens

1.7.1 Protection of privacy

Logged by operators who run the digital systems and picked up by sophisticated sensors in monitoring systems, the digital trail left by everyone, wherever they go, can make far more detailed data files than the traditional files compiled by bureaucratic administrations.

With these techniques we reach a whole new level and individuals can no longer keep in their own possession information about them which they do not wish others to see. Surveillance and GPS tracking techniques pose formidable problems when it comes to protecting personal privacy.

Objectively verifiable data was previously compiled and managed with specific and known purposes in mind. Now, however, the data-gathering system operates 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.

1.7.2 The right to opacity, omission and disengagement

Everyone should have the possibility of retaining an area of obscurity, in which they are able to remove all traces of themselves, to disconnect from the network, to disengage from infrastructures. Faced with the possibility of exposure of parts of their existence which they do not want revealed, everyone should be able to assert their right to a certain protective opacity. Currently data is being disseminated, supported by social networking practices and legal or pirate copies of data between sites. This dispersal makes it impossible to erase all traces. However, each individual has the right to opacity and to erase data in accordance with the known data retention period.

Indeed, web-based monitoring, the possibility of being traced via mobile phone signals, and, in the future, the monitoring of objects through radio-frequency tracking devices or through new internet-based functionalities expose the individual without them even necessarily being aware of it. Automatic identification, using IPv6, will allow everything to be registered, movements followed, and communication with others organised, so long as there are suitable sensors and interfaces. This opens up an infinite universe: the internet of objects. To forearm themselves against the undesired usage of their persona data, everyone should be told what data has been collected on them, what happens to the traces they leave behind, and whether they can be erased or retained. Certainly our contemporaries, particularly the younger generation, have little awareness of how potentially dangerous this irrational immersion in the digital universe could be.

Think-Trust encourages work to be done on technical solutions which will allow everyone to protect data relating to them. It also encourages Europe, and its constituent States, to strengthen the independent data protection authority that institutes and ensures compliance with regulations, in the same way that those governing road traffic allow us to travel in the best possible conditions.

1.7.3 Managing the life cycle of information and secure data formats

Through the information society, individuals constantly generate this raw material, information, relating to themselves, their past, their career, etc. Even as creators of this information they do not, however, acquire any rights or guarantees over it. It is at once held, managed and controlled; it is potentially shared with third parties, who may variously be a single entity, easily identified or may be an unknown quantity, or potentially a multitude, and may go so far as to be freely available on the digital network.

This change calls for personal control by everyone over their data, at all stages in the life cycle of this information. One approach could be a dedicated, personal, over-writeable network, in which everyone would be able to control data concerning them. Another perfectly feasible solution would be to create tools capable of destroying (or "putting in the

trash can", to borrow a current computing analogy) personal data about us which may be on the information network and thus exposed to all third parties. From the point of view of the data lifecycle, tools would therefore be needed which can deal with data at the end of its life cycle, through a personally-appointable collector.

1.7.4 The security of personal (hardware, software, data) cybersphere: the digital objects' life cycle security.

The scenario of nomadism (see 1.8 below) reinforces the need to achieve a mastery of the life-cycle of information and its secure media. An individual becomes, through the information society, a constant producer of this raw material: information on him, his past and his life-path. Being a creator of information does not give control of a personal cybersphere, neither automatic nor guaranteed. There is an involuntary sharing that results in loss of the creator's control of retention and management of dissemination, access and usage. It also results in unaccountability where the *shared* information may be attributable to an identifiable third party, possibly reduced to a single actor, or to a misidentified third party, or to a unspecified multitude, up to a situation of free access across the digital network

This evolution requires for a check by each on their data, at anytime during the life cycle of information. One way could be a personal dedicated overlay network, of which each person would have control. A potential solution would be also to provide tools (such as garbage collection in computer memory for object oriented language) that could go and destroy (or "put in the trash," by analogy to our computers) the information that is private but exposed to any third party. In a lifecycle perspective, it would thus be tools capable to ensure the final phase of the information cycle by a garbage collector activated at will.

1.7.5 Clarifying the roles played by ICT players.

This move will better determine everyone's respective responsibilities and duties with regard to security (telecommunications operators, network managers, content and service providers, etc).

The more of these players there are, the more support there will be for providing sufficient mutual or collective security.

One possible option is the virtualisation of everything which is currently represented by packets, routers, lines, bandwidth, sessions, etc.

A second key issue is that the balance of power between provider and user needs to be restored, especially when it comes to the individual user. It is currently very unequal, as the provider has a power which, in law and in social terms, could be described as an opposition force. Any failure to restore this balance in favour of the users, their usage, their access and their control over their own digital domain and the network will impede the effective development of practices, including any future commercial power.

We need to be able to devise viable forms of governance for the individual's infosphere: forms which can support their growth during mass deployment, and can extend to hundreds of millions of users. This includes the management of our data and the traces we leave behind us on the network, and also brings into play any solution based on the ability to audit what happens on a network to identify movements and entry points, whilst mainlining sufficient levels of digital privacy for all.

1.8 Mobility issues in a scenario of nomadism

1.8.1 User security here and now: its fragility, its dependence and the "big brother syndrome" in locating individuals.

Nomadism (intermittent connection and session from various locations) or mobility (continuous connection to a digital infrastructure and activity during the move) destabilize the perennial framework within the personal cybersphere security when the position is static. The security of mobility requires an anchor of geography and time. Nomadism and mobility especially emphasize the logic of a spatiotemporal security framework based on the *hic et nunc* (Latin for "here and now).

The concept of geographical territory, where legislation applies, retains its relevance in the sense that it remains necessary for the common safety, to report, through it, an act committed by an identifiable author, but also at the point of entry space from which the actions have been initiated originally.

The "now" introduces and facilitates an *in vivo* (Latin for “within the living") environment, which corresponds to the ICT specificities: capacity of near-instantaneous, customization capability, interaction or adaptation to a person.

In order to protect this volatile mobile digital life, made in real time and in vivo, several axes are possible:

- Protect our secrets and our identities in terms of identification and authentication, with tools and components such as secure USB keys, smart cards, SIM cards. It is to secure on the one hand, the individual, and on the second, the digital instruments of the person. This would be very useful for those who are engaged, while nomads, in connection with a playful or collectively online videogames with multiple players or multiple parties.
- Develop a contextual security, ambient intelligence, to deal with problems such as:
- Tracking, monitoring and traceability of people on a territory, according to their trajectories, refined observations of behaviour (eg through a crosschecking between input position and images of networks of urban cameras). This monitoring may be as much a source of protection, to validate remote access by an individual by introducing identity requesting such verification, a source of insecurity if violating for her privacy;
- Usability of security tools, awareness of the security of the user, the definition of a fair level between a sophistication need of protection in order to make its activity dependent on an awareness of its user, with capacity for him to disengage or configure these functions at will and desire of that user to a transparent, simple to the extreme, without activation. The good level of usability requires an arbitration with both technical and citizen orders;
- Mastery of consequences arising from this extension of itself that is the computer science tool, when this tool is likely to breakdown, malfunction or malicious taking control. There is a risk in the situation of dependence on both physical and psychological integrity of an individual to keep this tool a part of its memory, its links with the past, with the outside world, and particularly in need of communication, in crisis situation, etc.
- Provide tools and means to ensure privacy around personal objects: this affects in particular the Internet of things, and the fact to delegate our security to external entities: robot, micro-robots (medicine, digital prosthesis) or other artifacts. It raises the question of delegation (to whom, for what) for objects of our daily lives such as our car, in a multiparty situation (vehicle owner, repairman, car manufacturer).

For these objectives, it seems possible to prefer a type of trust infrastructure, rather than of a security infrastructure.

1.8.2 Redistribution of responsibility in the chain of actors involved in exchanges

In a situation of mobility, it is necessary to facilitate and clarify the roles between actors of ICT, to better identify the responsibilities and duties of each player (telecommunications operators, network operators, service providers, content or service providers, etc.). The issue of maintaining a mutual or collective security should be strengthened, as the number of these players tends to grow.

One possible way should be through security at the virtualization level: virtualization of all the paradigms (packets, routers, channels, bandwidth, sessions, applications, etc.).

A second key point relates to the necessary rebalancing of the relationship between supplier and user, including the individual user. This unequal and unfair face-to-face relationship is today marked by a strong asymmetry, where the provider has a power, in law, which results, in social terms, a power imbalance. A shift in this balance resulting in the enhanced usage, access and control of the user over their digital sphere will ensure development of uses, including their commercial viability.

It is important to achieve sustainable forms of governance of the user's infosphere : forms capable to support growth in the massive deployment, to the scale of hundreds of millions of users. This comprises the management of our data, the traces left on the network. This pertains to any solution based on an ability to audit what is happening on a network to identify trends and points of entry, while maintaining a sufficient digital privacy for everyone.

However, it is questionable whether the in vivo might not lead to a creeping form of *in vitro* (Latin for "Within the glass"), in the sense that the digital space of a person may raise as much of a field of freedom, by a form turning to his disadvantage, a field of monitoring and observation of facts, gestures and movements, even our opinions.

1.9 Identity

1.9.1 An initial classification for identity and personal data

The main issues might be analysed on the basis of a breakdown of functions or tasks likely to be carried out by computer systems. The following list is neither exhaustive nor set in stone. It gives us the opportunity to rethink the basic functions of computer systems which are ubiquitous, constantly connected and endowed with a diverse memory capacity.

- Personal data, in the sense that it can reveal the name or other identifying information about a person (or even an object), such as address, date of birth, etc. It may also include banking (account no, etc.), professional or other information.
- Information which identifies an individual's existence: they may remain anonymous but are still acknowledged to be an existing entity. (For example, in our daily lives we do not need to know the name of a person we might encounter in the street to confirm the evidence of our own eyes and to start to form an opinion on them, decide whether we find them either helpful or unhelpful, decide to make a friend or enemy of them, etc).
- Information which defines them in terms of their consumer, philosophical, political preferences, etc.
- Information which tracks them spatially, without necessarily knowing who this person or object is (I may not know the name of a traveller, but I know where he or she has been, thanks to swipe-card, date-stamping and ticketing systems).
- It is worth mentioning that one could also previously speak of temporal traceability, which may involve looking at our educational record, our youthful opinions, etc.

The functions may therefore be summarised as: naming, designating (tracking without naming), psychological or behavioural profiling, following.

The current problem with legislature and data protection authorities is that they focus exclusively on the first issue only (nominative data), whilst the others seem to be growing as a result of interconnecting files, and data aggregation and collection facilities. Web2 and the most recent developments support this trend towards transferring private personal data into digital formats and in an open environment.

It is worth noting the position held by several German officials who have seen fit to tighten legislation governing the trading of files containing personal and similar data, often even threatening to outlaw it altogether. These decisions also extend to increasing the severity of fines for illegally trading data. This case also saw an embryonic atypical "economic model" proposed, with a minister suggesting that a company pay back any profits derived from this kind of activity.

1.9.2 Identity à la carte

There seems to be a broad consensus on the desire for flexible identity systems. This could take two possible forms. Individuals could have an "à la carte" choice regarding the sending and receipt of data streams:

- The ability to decide on the level of security of data streams concerning them (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 levels, only the aspects of identity required for that particular connection are revealed.

Following the accountancy model, based on a reliable identity, to be attached to an initial territory-based registration, it would be possible to temporarily abandon this reliable identity for a particular data stream or connection, but without being able to divest oneself of the rights or facilities which the recipients or operators might require from these same streams attachable to a trusted identity.

1.9.3 Examples of à la carte identity

There have been various proposals made regarding identity relating to the “just enough” approach to information transmission.

- A data stream/sender could be issued with a ‘travel pass’ type document, based on the idea of a transport ticket:
- for buses, it shows the destination.
- for trains, it shows, destination, seat, time.
- for aeroplanes, it also shows an identity, validated (cross-referenced) on presentation of a passport.
- Identity certification could also be based on ID-card-type processes (driving licence, passport, etc), which do not necessarily contain the same information.

These various approaches are often governed by the principle of sending to the recipient or intended recipient only what they actually require for their own part. For the other elements, they will be informed of the authority to which they should apply to obtain possible confirmation or further information.

1.9.4 Current example: secure electronic identity in Germany.

The recent development of social networks and blogs on the internet has led to a huge proliferation of personal data on internet users. Each of them has to manage a genuine “digital identity” made up of their contributions and the traces they leave on the web. The growing use of the internet by individuals, businesses and government entities raises the question of information security and personal data protection. In addressing this issue of authentication technologies, users are given the confidence they need to use the internet as a tool. To this end, the German government has decided to implement an electronic ID card system for all German citizens, starting in November 2010. This is meant to be able to prove an individual’s identity and to be able to give proof of objects and products, as well as guaranteeing intellectual property using innovative procedures such as watermarks and digital signatures. German R&D has initially been focussing on the following issues:

- Secure reciprocal proof of identity through the use of an electronic ID card;
- How will electronic identities influence how the average citizen organises their daily life?
- Secure identity: transparency and authenticity in the real and digital worlds;
- The use and administration of secure electronic identities;
- Long-term security and quality of official electronic documents using the leading smart-card reader family Infineon;
- Display technology for multipurpose cards;
- Time-stamped digital signatures;
- Digital signatures for VoIP communication;
- Digital watermarks for the authentication and protection of digital media.

1.10 Accountability

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 all networks, and such that reliable and more or less exhaustive incoming and outgoing accounts can be drawn up.
- Reintroduce, on a lower 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.

Other approaches have been suggested, and are worth looking at in greater detail; however, the two principal options mentioned above seem to have immediate unifying and organisational potential.

This two-pronged global accountancy and re-territorialisation approach could offer an alternative to the mutually opposing laisser-faire/network policing options. It could also buck the network trends towards ubiquitous practices, nomadism and varying identities.

On a more general level, a similar approach might consist of implanting time/space marker points into the system.

- The spatial could borrow from IBM's vision of an existing physical relationship between an internet user and an administration (or any ad hoc interlocutor) which could validate their real identity in a permanent, stable and guaranteed manner.
- With regard to the chronological dimension, the accountancy approach would require the temporal dimension to be implanted into the functionality of future tools. This is inspired by existing accounting practices, in which the principle of chronologically recording facts is not enough, and is completed *a posteriori* through the re-use of the same data in an incomings-outgoings system which has to balance up (all incomings and outgoings must be entered with their complement on the assets-liabilities balance sheet or as receipts-expenses on the operating account: this is known as double-entry book-keeping and guarantees, *a posteriori*, that the chronological records are accurate, that nothing has been omitted or added - inversely, the chronological record validates the overall balance sheet).

1.10.1 Towards a chain of "certainty" or "trust"

The chain principle is useful inasmuch as the need to continuously access excessive information (who, where and what?) is replaced by the knowledge of just one of these elements; access to the other elements then requires recourse to other parties and/or public (and also thus visible) procedures.

One of the potential applications of the chain system is the initial 'territoralisation' of the individual (e.g. the territory in which their passports was issued for real, physical travel). If the individual sends an email on the network from another territory, they can use this identity, which ensures they can be traced back via the entity in charge of registering their existence and issuing their digital identity.

1.10.2 Preliminary questions: the cost of insecurity.

By posing two preliminary questions we can start to define a framework for discussion of the two weak points in personal data protection, i.e. the lack security and of service quality.

1. How do we define what is intended by the term "reduction"? Is it a matter of eliminating undesirable situations, reducing them, or rather absorbing the cost of them without actually eliminating them? The logical extension of this would be to divide out the cost using an intelligent incentive-based system, although this attempt to effect behavioural change

applies just as much and for just as long to the drawing up of rules and regulations. The other term of "weakening" covers a range of possibilities: do we weaken the situation or its effects? In computing terms, this dilemma is very familiar: who negotiates between the effort to prevent a dangerous event occurring (the likelihood of it happening) and the effort to reduce its consequences (loss of data, delays, damage to reputation, etc)?

2. How is the exact cost of it to be calculated? Are we to have recourse to systems of measurement and evaluation on the basis of subjective or objective criteria? This issue highlights the difficulty of defining the notion of damage: what is it worth? Who is in a position to evaluate this? Should be down to the victim, the accused service provider, expert third parties in the courts, or insurance company experts? Estimating the immaterial dimension of damages is also a subjective process: justice has managed to reintegrate this point in its "economic model" as it is able to define fair financial compensation. Can we therefore do the same thing through other means such as amicable settlements and standard market ratings? Similarly, costs could perhaps be estimated through a supply and demand model, based on past records (historical cost accounting). Operating according to market regulations presupposes that "rational expectations" include future costs in the current price, but counter examples reveal the existence of weaknesses or loopholes which can be exploited by some economic operators. In a reversal the process of calculating costs based on past accounts data, what criteria will govern the conversion of future costs to current value?

All of these considerations point up the fact that superficial thinking will not suffice if we are to formulate a price-setting system which is honest and efficient from a socio-economic point of view.

1.11 A legal continuum between the material and the immaterial

Faced with this new situation, technological or political decision-makers have two choices:

- To consider that we are entering a world so new that the usual rules of society, including legal regulations, are inoperable therein.
- A second view is that all technological evolution, both materially and through the fact of it becoming a "social object", quickly becomes embedded in the existing social conventions, as largely dictated by: laws, conventions, recommendations, the rules of social engagement, moral condemnation of actions which impinge upon others' interests, etc.

The latter option, although it may not be immediately adopted, relies on three observations:

1. Observation of the material nature of the ICT sphere

Philosophically, those who posit a break with the old technological and legal world often rely on the notion that ICTs constitute a purely virtual world, which is not in fact the case, as the electrons, photons or electromagnetic waves which transmit this information are real, the magnetic devices on which information is stored is tangible; the "immaterial" (knowledge or identity) will long have need of the "material" in order to exist and to translate into a culture communicable to others. Legally speaking, a bit of information has an owner, even though it may not always be that of its repository (one can store ones property in a bank vault, without necessarily relinquishing ownership of it).

Will areas of absolute or relative non-ownership come to exist? Or perhaps we will see the emergence of co-ownership, or the subdivision of property into subsidiary elements in the same way that immoveable property is legally defined in terms of usus/fructus/abusus (that is, respectively, the discrete rights to use, profit from or destroy or sell an item)?

2. The premise of there being no legal caesura between the real and the virtual

The broad principles of law in no way prevent its application in the so-called "virtual world", as one finds therein legally well-defined ideas such as harassment, destruction of property (albeit digital) and intrusion of privacy. These approaches to the issue might tend to blur this virtual/real caesura,

for as far as the law is concerned, when it comes to judging damages and responsibility it is irrelevant whether data is written in ink or stored in magnetic form. This point leads to one of the subjects to which the Think-Trust is to contribute, namely, to what extent will the future internet be an essentially lawless zone?

Will there be areas in which the law does not apply, in either absolute or relative terms, or areas of co-regulation, as currently exist for ships outside of territorial waters, or satellites in space?

There seems to be nothing in the current legal apparatus which prevents its application in the so-called virtual domain. However it is inevitable that there will be a phase of adjustment, perhaps even experimentation, whilst the law gets to grips with the specifics of the future internet. We might attempt to classify these specific characteristic in the following way, which, albeit reductive, serves to throw the main issues into relief:

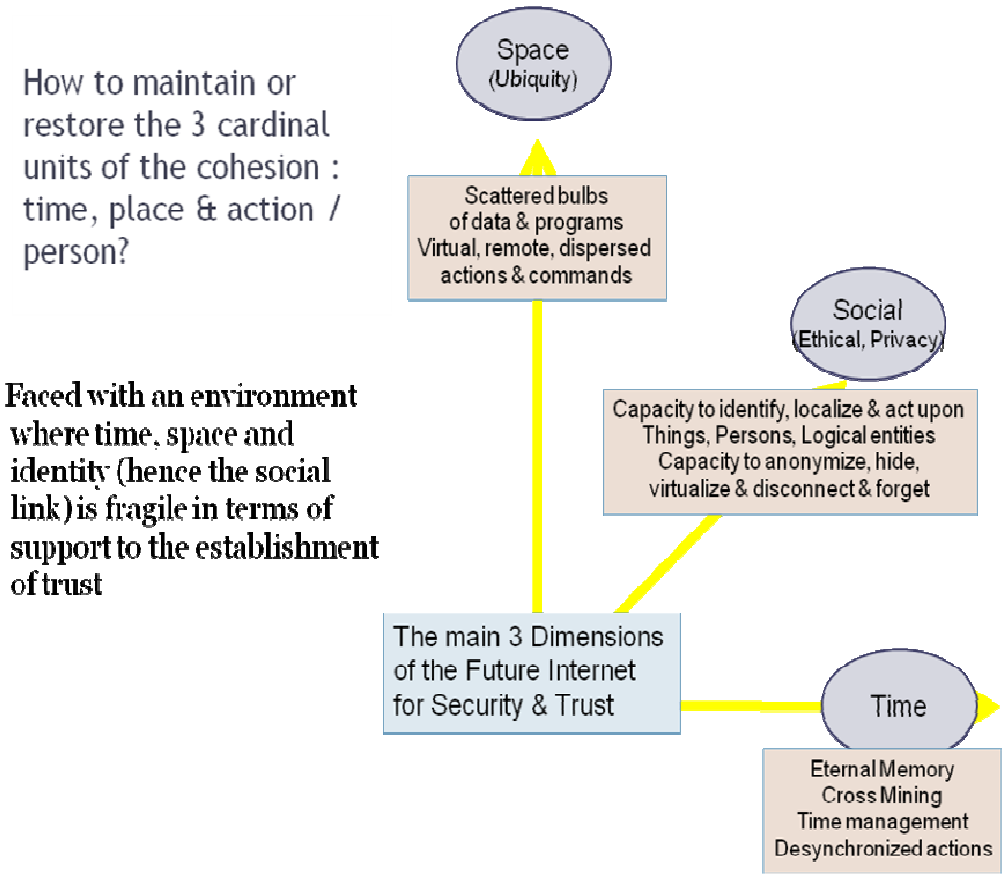

Figure 2: The three dimensions of the Future Internet

This diagram shows that the law may for example apply to uses relating to immediacy and spatial dispersal (e.g. an individual based in one country but possessing electronic data in another, or having programmed an action from a third). This does not necessarily require new laws, but rather working with case law to apply the fundamental principles of law to technological applications which make actions quicker, more disparate or fast-moving, and whose origins are less easily attributable to a specific entity.

3. The trend towards the normalisation of dissident actions over time

The hypothesis of the “normalisation” of the internet over time is borne out by observation of previous technological revolutions: the Gutenburg press gave rise for over a century to multiple copyright infringement actions, one notable typical example being the fact that the French writer Corneille saw numerous pirate copies of his works published during his lifetime, one by a Dutch

publisher which is still in existence today and which is now a law-abiding market operator. Similarly, cinema in its initial format (film), was initially subject to numerous copyright infringements; this was indeed the case in the 1910s, for example, to the detriment of European films shown in American cinemas. The film industry has now become a fervent defender of the law. We can expect to see a similar trend with the internet, so long as there is support for it.

It is on these means of support and assistance that the Think-Trust is to focus. To this end, we consider it useful to initially create a set of "conceptual tools" which can be used to draw up general technical specifications for future communications systems.

1.11.1 Forming new concepts before defining legal and technological solutions

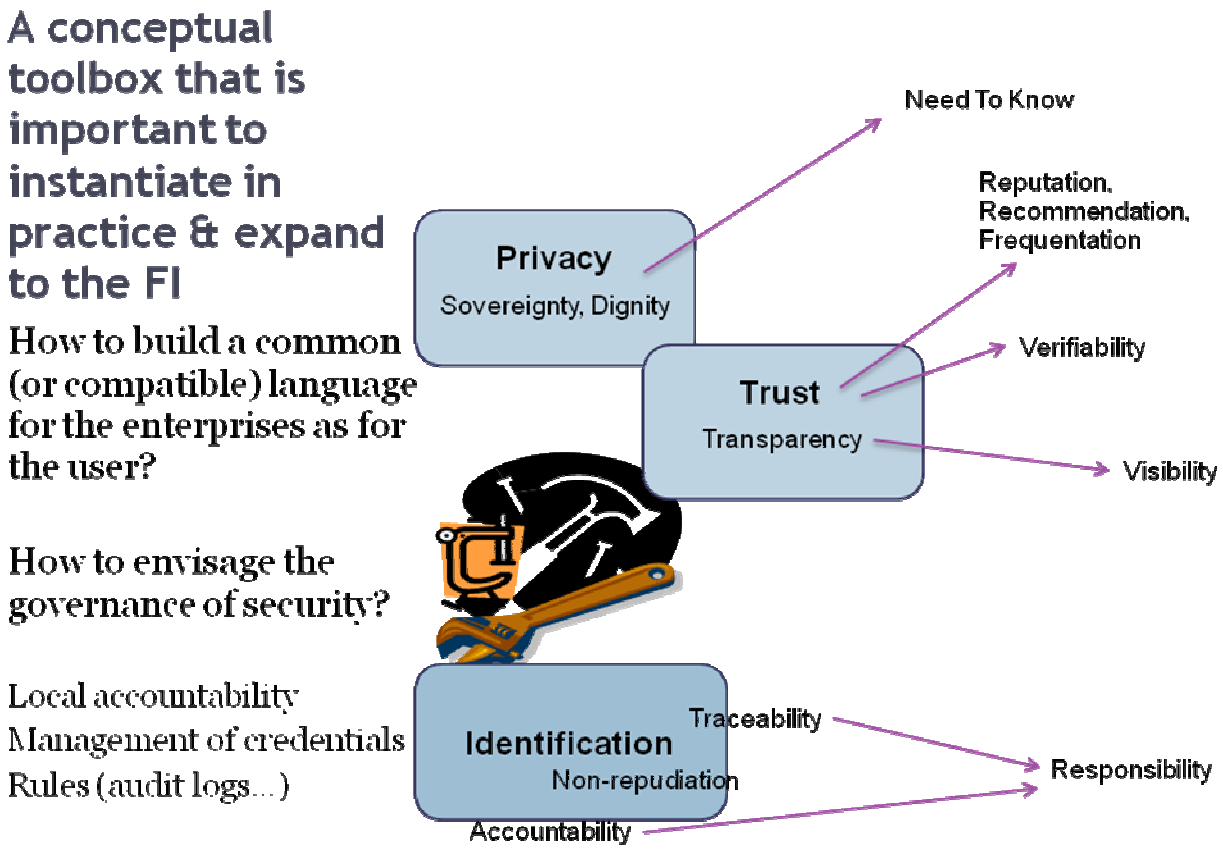

Figure 3: A conceptual toolbox

Several of these "conceptual tools" are already well-known: notions of privacy, confidence, accountability, transparency, individuals' right to privacy and personal data protection (with the personal digital domain itself liable to become spatially disparate, aggregated or superimposed with other personal or business domains, e.g. online management by software publishers of certain programs installed on our computers). The term "domain" implies that we are dealing with a homogenous, concentric entity, whereas it might be more accurate to describe it as sprawling, capillary or porous.

1.11.1.1 Modest beginnings inspire confidence

It may be possible to combine these "conceptual tools". Similarly, by making the connection between confidence and transparency, it is easier to then define the idea of "visibility": exactly how

visible can any citizen's interlocutors, equipment or connections really be said to be, (in terms not only of security but also the relationship between appearance and reality)? Visibility is different to transparency in that the latter is supposed to be exhaustive, posited as an ideal, whereas the former is more concerned with ensuring a sufficient level is reached to inspire confidence: is the visibility of other individuals or equipment sufficient to inspire my confidence and allow me to communicate with them?

This idea of visibility leads to the need to attain certain thresholds, in two senses:

- How much and what kind of information do I need on my interlocutor or equipment to "function" in the sense of having enough confidence to interact with them?
- Conversely, how much and what kind of information do my human interlocutors or hardware interfaces need about me to "function" with me?

This focus on "thresholds" can lead us in a number of different directions, often influenced by cultural factors. In the Anglo-Saxon context of interpersonal and private contracts, it might be a matter of reciprocal and comparative thresholds: which of the two correspondents agrees to the greatest effort to become effectively transparent but simultaneously not demand too much unnecessary transparency from the other? Who assumes greatest responsibility in the event of a mistake (such as losing a file containing personal data on a partner with whom one has corresponded) or a breach of confidentiality (for example the selling on of collected private data). From this point of view, a threshold would partially become a relative value, both in relation to that of the other and from the point of view of fair distribution of effort. It would be best described in English as a "fair" situation, in which there would be an element of accounting to accurately assess the situation, particularly so as to be able to quantify each party's contribution. This would thereby calculate any possible deficits on either side.

There are a number of other possible approaches, which might involve the formulation of either a subjectively-determined minimum confidence threshold (independent of the other party's threshold or any possible effort on their part if they start from a low level), or a desire for objectively-calculated thresholds. This would require recourse to adjudicating third parties and would constitute another version of what is known as the "social contract": I defer to a designated third party who will defend and represent my interests and then determine the rules instituting rights and obligations for all, including me.

Both the private interpersonal contract and the social contract will undoubtedly be very much a part of the ongoing debate on the future internet.

Visibility demands a definition of how this is to work. There are various possible solutions:

- One approach proposes a straightforwardly declaratory method: a site or software publisher will make public their security policy, ethical and behavioural policy, and how it is implemented in their products and services. This nevertheless implies the existence of a favourable environment:
    - The existence of moral pressure on the declaring party, emanating from civil society and pushing the criteria for honest disclosure to a higher level. There are a number of considerable cultural disparities on this issue. The USA, for example, favours this overall approach, placing as it does greater cultural importance on public declaration (contrition, repentance, pardon, declaration of good faith, swearing before a jury, the grand jury principle, etc). The quasi-Biblical attitude behind this does not exist or is markedly less prevalent within other cultures, which value more individualistic behaviour, or, at the very least, are less communitarian in the Pilgrim Fathers' sense of the term. Of course there are also certain countries which are influenced by criminal organisations but which are home to many good software publishers as well as pirates.
    - Generally speaking, this approach has no other value than that contained within the declaration "I swear to tell you the truth by declaring that I shall not lie".
    - An effective and deterrent system of sanctions in the event of fraud. Currently, those cultures which place little value on the public declaration lack such sanctions.

    - A system which informs users of the existence of fraud, and gives them adequate "publicity".
- An intermediary model, in which the declaratory principle is set within a framework of technical specifications stipulated by independent bodies. However the inadequacies inherent in the previous system are also seen here, as the question of veracity, sincerity and moral obligations remains the same.
- Another intermediary model is based on joint or corporative structures, as much to enact constraints on declaration as to add an additional level of professional verification and sanction (in the same way that health insurance companies employ examining doctors). However this presupposes the existence of organisations which are virtually non-existent in the current IT environment, despite their prevalence within such self-regulating professions as law and medicine in various countries.
- Other approaches go beyond the declaratory model to suggest direct user verification or having intermediary private or public bodies perform this function (as exemplified by the certifications provided by private control bureaus for oil tankers, although they have been seen to carry the risk of complicit circumvention).

1.11.1.2 The optimal adjustment of mutual recognition for all parties

The "visibility" philosophy links to a whole range of pre-existing concepts, one of which is taken from strategies for "just in time" or "just enough" manufacturing logistics, viz: it is as unnecessary to deliver (items or information) in too great a quantity or too early as it is too little or too late. Applying this concept to network data, the issue might be summarised thus:

- What is my personal confidence and communications threshold?
- What is the confidence and communications threshold of my partners, suppliers and other relevant socio-economic parties?

In many respects, this idea relates to the "need to know" principle, which is similarly based on the notion that total disclosure is not necessary for an action to be carried out or contact made. This calls for a more precise theoretical definition of transparency (e.g. legislative and legal) and for it then to be specifically applied, thereby making it operational.

Opening and holding this debate presupposes the need to define key concepts, foundations for future decisions:

- How do we define the idea of digital capital?
- More generally, how do we define digital citizenship?

1.12 Trust

1.12.1 Instilling trust in the digital ecosystem and keeping it in a robust condition

The galloping digitization and computerization of the modern world is pushing towards the generalization of networks; this generalization is carried along by new concepts such as pervasive networks, and ubiquitous computing or ambient computing. These new tropisms are highly heterogeneous both in terms of policies and technologies deployed.

From the security point of view, this heterogeneity tends to increase the complexity of the main security functions, like identification, authentication, access control and data protection. The implementation of these functions usually follows objectively from a trust model in the form of a trust infrastructure, itself forming the basis of the security architecture. Trust is thus at the heart of the security because the necessity and pertinence of the deployment of some other security mechanism depends on its existence and on its level or characteristics, and reciprocally.

The absence of a measurement of trust in digital systems is one of the major obstacles in the maintenance of networks and telecoms infrastructures in a controlled state, both in terms of security and reliability of operation.

The lack of trust in ICT infrastructures shows itself at every stage in their life cycle: during operation, because these systems have to confront intentional attacks or cope with accidental breakdowns, and at the design stage because security or robustness are often not included in the system's specifications.

Communication infrastructures and systems involve thousands, even millions of nomadic devices and the implementation of virtual constructions (virtual networks, overlay networks) which operate both on the hardware and the software, and on the network and the servers.

Security architecture constitutes a beginning in the treatment of security in heterogeneous networks. The completeness of the specification of this architecture remains an objective to be reached; an objective of which the satisfaction is dependent on the raising of a number of questions and limitations.

Beyond the security of the trust model which has proven to be an essential element conditioning the security of the overall security architecture, are other questions, likely to put this architecture at fault. All the aspects and questions broached represent stages to be cleared or at least to be dealt with, in the achievement of a platform simulating our security architecture.

It is advisable to automate and make the trust infrastructure more dynamic through interaction with the security infrastructure, so that authorizations, exceptions and the general security management are carried out by the system itself. Such is, in substance, the objective of this trust platform. The objective is to accompany and strengthen the security and reliability of the cyberspace, the ICT infrastructures, networks, services and systems. Research will be interested by trust models in general:

- the definition of trust: total, partial and assigned trust;
- protocols for instilling trust;
- the range of trust models (based on reputation, frequentation or surveillance, on security or redundancy mechanisms) with regard to a system, a service, a network, a hardware or software component, or an architecture.
- the variables to measure trust in real time in a system;
- the estimation of trust by a user, an operator.

The construction of a trust framework must offer a hybrid trust model for heterogeneous networks (heterogeneous primarily though policies) in which one leans in particular on its distributed consonance; a consonance inspired by the social trust model and based in its formalism on heuristic mathematics. One will thus be able to experience the contours of a new security architecture with a design crystallized by its close links which unite, without dissolving or mixing them up, the trust infrastructure with the security infrastructure. Furthermore, this new architecture will take into account the heterogeneity of technologies as well as the heterogeneity of policies. The searching of data or rather the communication of various data relating to an entity of which one wishes to gage the "trust" can also play an important role. In everyday life malicious people are often betrayed by "shady" details which they have forgotten, or have not been able, to mask.

1.12.2 Trust versus security

1.12.2.1 The distinction between Security and Trust

We have to distinguish between the various following ideas:

- Security is a non-functional property of a component, a system or a service;
- Security assurance of a component, a system or a service, which is the quality of the design and operation of this property, is the degree of trust in the system's security, but not necessarily the degree of trust in the system;
- Trust (or distrust) expresses the quality of the relationship between two entities; these entities can be persons, physical items (components, equipment) or intangibles (virtual machines, software or data files).

Certain titles (trust infrastructure, trust operating system, trust module etc) confirm the confusion by mixing up the two concepts of trust nod security, or more frequently the concepts of trust and security assurance, which in no way helps in understanding for non-specialists.

For example, so-called trust infrastructures such as PKI are generally not trust infrastructures but rather secured infrastructures (for key management). Indirectly, through authentication of the entities, they can instill trust in a digital system in which no one knows with whom they are in contact. Such infrastructures generally have good security assurance (they bear a quality approval), which does not mean they must necessarily be trusted.

"Trusted OS" are secure operating systems that properly execute the tasks they have to carry out, usually through compartmentalization. They do this with primitive security functions that can be used by the applications. Their guarantee is security assurance. However, they cannot necessarily be trusted.

For marketing purposes, the TCPA alliance has been called "trusted", but the specifications in no way provide trust for the user. On the contrary, these are systems the user should fear, because they take away from the user sovereignty over his system and data. Similarly, the TPM (Trusted Platform Module) of a user's PC's motherboard can be assessed using the EAL3 Common Criteria, which does not mean one can have trust in one's own "personal" computer.

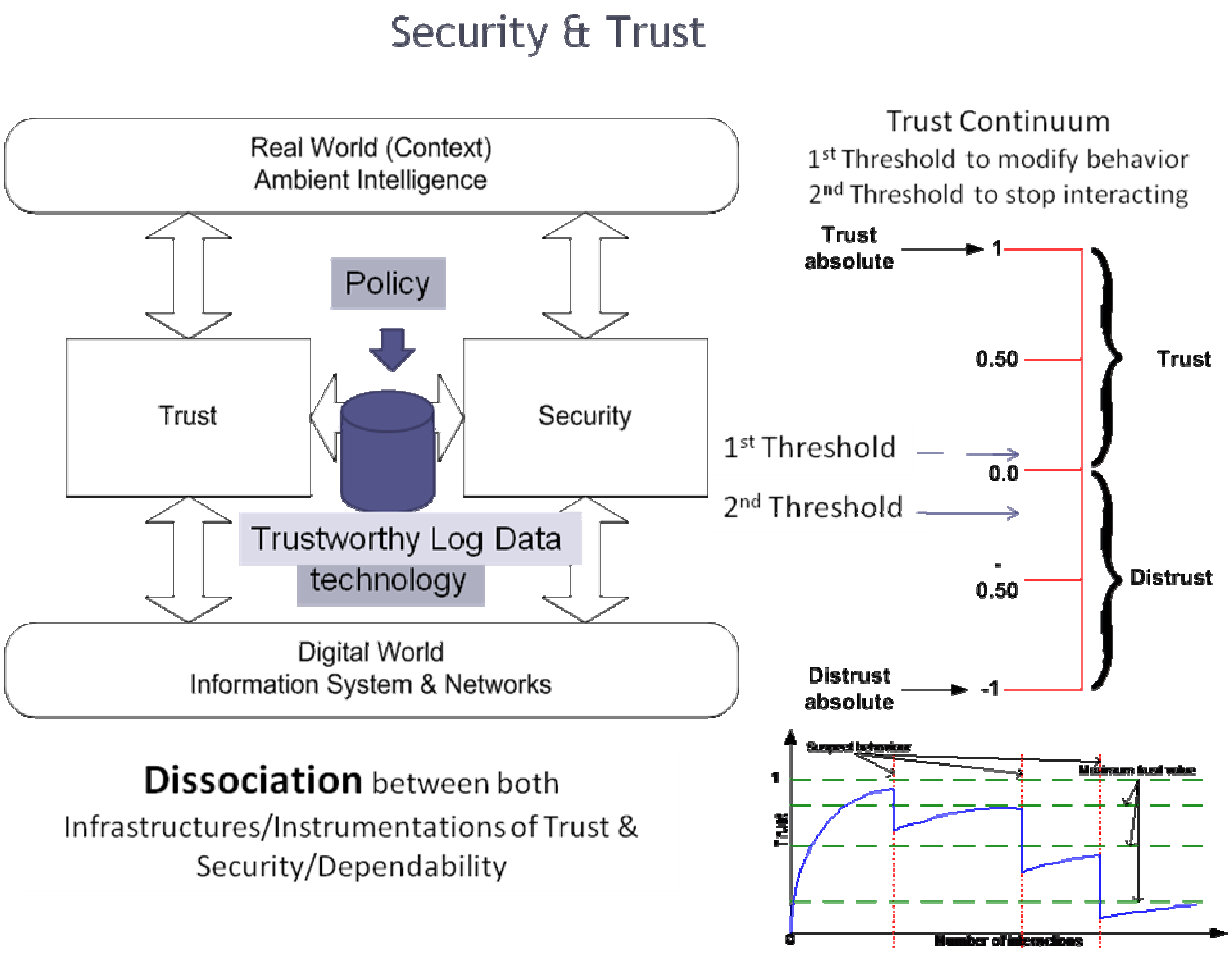

Figure 4: The Distinction between Security and Trust

1.12.2.2 Security functions associated with an entity

The following, various functions must also be distinguished, which are frequently badly defined, poorly understood and wrongly interpreted in security literature:

- The identity, name of the entity or alias (and the associated authentication, accountability and non-repudiation functions),

- The anonymity, masking of identity, unawareness of the person's name, and thereby the absence of responsibility, because it feels authorized to do everything (spread viruses and spam);
- Traceability (and the related functions of reporting, flagging and surveillance),
- Disappearance of the entity (drops out of sight) and the loss of identity; the entity and its name have been destroyed or have simply melted into the immensity of the IT magma, to reappear at a given time.

There is sometimes confusion between the use of identification and the operation of authentication. The latter can prove the identity of a person or prove the tracking of a flagged but anonymous person, or the behaviour of a software entity that has been flagged but for which the relationship or link to a responsible person is unknown.

More than the function of identity, the traceability function is increasingly important in this mobile universe. Anonymous persons can be traced. Accountability and responsibility are crucial in this digital world.

1.12.2.3 Reminders about security and security assurance

Operational security can take the form of models for protection, dissuasion, survival, deception, disinformation, crisis management and attacks.

Faced with threats (limited or vague, known or unknown), operated by enemies or attackers, faced with breakdowns and the fragility of the system (due to poor design or sensitive operation), and with a view to get the most out of the IT assets (services, software, files, brands on the web etc), a manager (either a person or a body) defines a security policy that is implemented using security functions. Security functions (identification, authentication, access control, auditing, data protection, communications protection etc) are implemented to achieve security objectives that can be expressed in terms of confidentiality, integrity and availability.

Security assurance is a measure of quality (in the general meaning of the term) of the implementation of this security, in the design, operation and use of the system. It is an assessment of the strength and correctness of the mechanisms implemented, measured by taking into account the entire life cycle of the system, from design to destruction.

1.12.2.4 Trust consideration

Trust is a different concept. Generally it has nothing to do with the security of a system, even though of course there is a relationship and a link between the two concepts.

The security of a system is an intrinsic, non-functional property, outside of any other entity, like upgradeability, flexibility and manageableness.

Trust in a system or its various sub-systems is a property of the relationship with an entity (for example, myself) that does not belong to the system or this subsystem Trust is a binary relationship between two entities that are going to interact, not necessarily in the same manner. This entity is a person but can also be software, or a virtual entity.

The degree of trust or distrust in a system will define a strategy of thought, decision and action in respect of the system.

In practice, everyone defines their confidence based on trust models. It is a mutual relationship that depends upon the context, and frequently on the history of the relationship between the two entities. It is possible to define this trust relationship between two entities using a mathematical function. The underlying trust model is a relationship built on:

- Ontologies (by definition and construction of the entities, they satisfy the trust function that varies as a function of time, space and context);
- The construction of entities based upon one's physical inspection (I have examined the software source code, it does not necessarily do what the specifier wanted, it does not necessarily do what is stated in the documentation, but the software is on the one hand not

aggressive and on the other hand not vulnerable, meaning it can resist certain attacks, but will not be able to resists in such and such a context such and such a menace.

- Experience (following a history of interaction, through behavioural analysis I believe that a trust factor can be calculated and inferred);
- Acquaintance (I have used it for a long time, it works and has never let me down, so I can trust it in the future);
- Reputation (many people that I do not really know have told me that I can trust it);
- Recommendation (not many people, but they are trustworthy, have told me I can trust it).

1.12.2.5 Measure of trust

Trust is a non-reflexive, non-symmetrical and non-transitive relationship. Mathematically it is a lattice that does not create a total relationship but only a partial one. Within this group of values there exists a greatest lower bound, a least upper bound, but in general it is not possible to compare two trust relationships.

Trust in a meta-system, within a system, an infrastructure, a service, an application, software or hardware, a product or a component, thus depends on the trust policy that one has defined for oneself and that develops as a function of time, space, context and history. Trust functions are very characteristic functions in terms of time (trust has difficulty growing fast, but in general decreases very quickly, for example following some event). Having been let down, the entity will have difficulty building trust back up quickly and it will not reach the level it had been at, unless there is an element of forgetting involved.

Trust varies from –1 to +1. Negative trust (distrust) is relatively common: one does not have trust, but the policy says that one can act in any case. Positive trust (>0) facilitates acting more or less. Blind trust (=1) is dangerous. The exact assessment of the degree of trust is not very important. What counts are the two basic thresholds in this gradation. What counts in trust is less the absolute value of this trust than the two thresholds, C1 and C2.

- The first threshold, C1, is a value below which one will change one's behaviour by being careful and vigilant. From threshold C1 I change my view of the system and I will act differently.
- The second threshold, C2 is a smaller value, below which of one's own free will one puts an end to the relationship (for a certain period of time). From this other threshold, C2, downwards, I stop interacting with the system.

Depending upon whether one is optimistic, aware, in a hurry or pessimistic, paranoid etc, these two thresholds vary. These thresholds vary as a function of a sometimes uncertain context: an atmosphere that can be described as warm, courteous, suspicious, malevolent, hostile, according to which one has with the other complicity, a well-intentioned attitude, perplexity, a careful attitude, increased vigilance, a violent reaction.

In a commercial context, for small stakes, I make fun of the trust I can have in the system: happen what may, what counts is what I do, because if what I do is seen, falsified or stopped it is unimportant, it makes no difference. The risk is worth it, I need to act.

In a highly sensitive context, what counts is to do something, but fully secure (in terms of confidentiality, integrity and availability): the message must not be divulged, it must arrive at its destination complete and correct, and the route must not be blocked or interrupted.

In an open world, what counts for the user is sovereignty over his digital universe, over his personal domain.

In a malevolent and even hostile world, what counts for the user is the dignity of software and content.

1.12.2.6 The composition of trust

Measuring the trust of a component or a system is not easy for two reasons:

1. Firstly, it must do what it is meant to, and develop this function through use;
2. Then the difficulty is to accumulate these trust values within an IT structure.

In IT the vulnerable objects are in general composites. Is this the case, for example, with a session? A session is quite an abstract ontology with the servers, the OS and the network for support. How do you put together the atomic values of trust to calculate the trust of a session?

In IT, objects are dependent on each other. If trust in the network is 0.8, 0.9 in the application, 0.7 in the operating system and 1 in hardware, what is the end-to-end trust of the service. On the one hand the trusts C1, C2, C3 …Cn must be considered, and on the other hand the dependence between mutual trusts C12, …, Cn-1, n.

If an application (C=1) operates on an OS (C+0.5), what is the trust of the entity being the application on the OS? The minimum or center of gravity [C= (C1 + C2)/2]? Unfortunately, the commonly held idea that the trust (or security) of a system is equal to the trust (or security) of the weakest link, is in general false. We in fact create system architectures, made up of related entities, exactly in order to increase trust in the whole (through redundancy) or to filter the dubious parts: the reason an institution has procedures is to clean up the items created and the output that lacks trust. An individual can make a mistake, which is not the reason his or her institution will endorse the decision or output of its employee. A real time system produces results, which does not mean that the system will take at face value every statement of this entity.

So trust depends a great deal on the topology and geometry of the system.

Thanks to routing protocols and network architecture, we can greatly increase trust that we have in a system, even if its internal components do not necessarily have high trust (a virus attacker implements a multi-part policy to create denial of service: statistically this will end in success for him).

1.12.2.7 The instrumentation of trust

The idea therefore is to weave a trust infrastructure over the digital system to allow each user or every sub-system that interacts with another to decide in full awareness whether the interaction can take place, So we are going to calculate a network that at each point will calculate the trust to be obtained, In the light of this, each person will decide if they can act or not.

1.12.3 Security policy and trust policy

There are interactions between security and trust. If trust reigns, security measures can be lighter. If everyone has trust, the security policy will be to do nothing and protect nothing. If there is no trust in anyone or anything, there will be tyrannical, ostentatious security, which will simultaneously react and (perhaps) create trust in the system, at least at the beginning, but then things deteriorate because entities do not adjust well to dictatorship or terror.

If security measures are strict they might be effective, and then trust can be created; or they might be ineffective (it means nothing, it is just the manipulation of public opinion) and in that case there is trust but it is overvalued and places the citizens in danger.

In general there is a dynamic relationship: security measures increase trust in the system, and a relationship built on trust will lower the security measures. There is thus a dialectical adjustment to minimize costs and the disturbance caused by the introduction of security measures.

1.12.3.1 The link between security and trust

We must accordingly distinguish between the two concepts of security and trust. The two infrastructures, the systems and the instruments must now be separated, those that serve security and those that serve trust. Now in the networks and the systems there will be tools and algorithms to create, manage and maintain trust in a system. And by the way, protection systems will always be created (encryption of content to protect semantic content, a firewall that protects access to a system's frontiers through access control), as well as security (digital tattooing of content to dissuade a pirate from copying and using software).

Obviously, and here things become complicated, there must be, in the traditional way, security assurance for the security infrastructure (these are the classic assessment methodologies for security such as ITSEC and CC), and the trust infrastructure must be secured. However this is a less important aspect of our thesis, because it simply involves securing one service like another, with good service assurance.

IDS and IPS are often systems in which security and trust are mixed together. Data is collected and the variables calculated, which facilitate deciding according to behavioural models (normal, not normal) whether or not an operation is legal. This in fact involves the underlying introduction of a trust factor that facilitates deciding yes or no, about performing a transaction or certain traffic over a network.

1.12.4 The security crisis: the parade of trust

Today we know that it is not possible to protect a large, open, interconnected system with mobile components. Thus to secure it, other means of protection are employed. In place of protecting there is prevention, repression, user awareness, attackers are dissuaded and tricked … and the law will try to do the rest.

You cannot wrap every mobile object in armour, all the more so since in general there is a reduction in IT energy at the periphery of networks. So it is preferable to save resources for positive functions or ones with added value, rather than to waste them on counter-productive defensive measures.

Faced with this crisis of security tools that is more favourable than that of a closed club that has to open up to the open, mobile, interconnected world, the idea emerging these days to make progress is to improve the Defence process with a more complex and more local decision-making algorithm, to substitute the idea of security that defines the state of a place with an ersatz Defence, namely the idea of trust, which will feed and support the decision-making and action process of the entity that is acting on the system. Instead of protecting the system, we will measure the trust that can be had throughout the system, or at least in the sub-systems with which we plan to integrate.

1.13 Economical aspects

1.13.1 Integrating weaknesses and the cost of their reduction within a coherent economic model

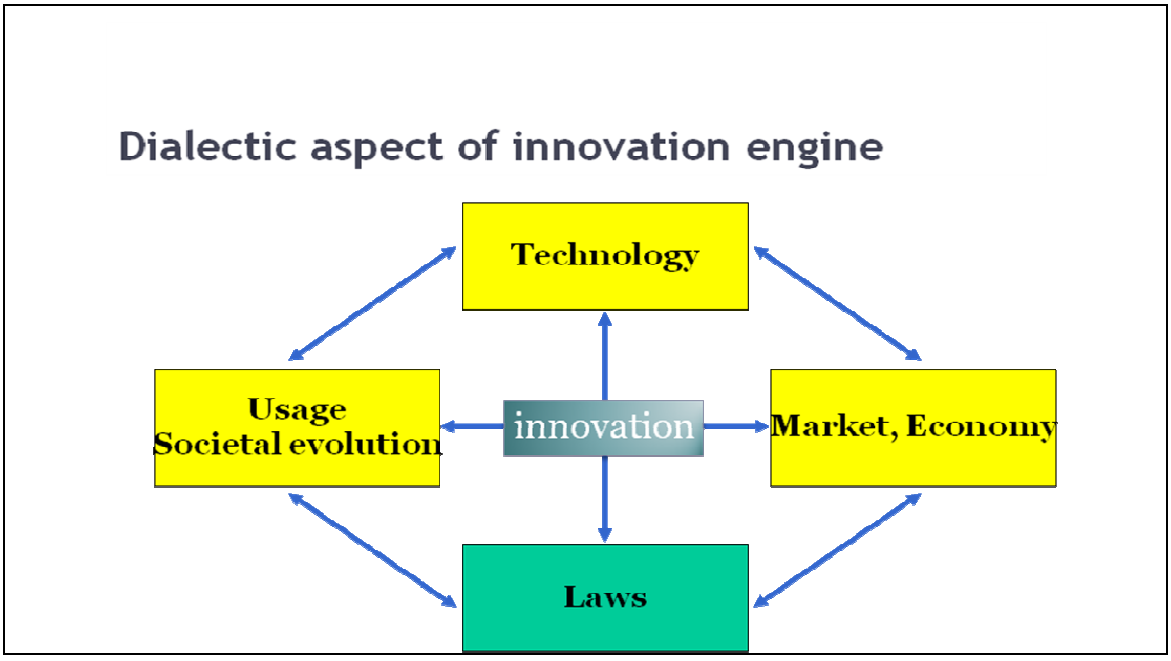

Figure 5: Dialectic Aspect of An Innovation Engine

Firstly, it is commonly observed that it is difficult to incorporate security, in the broadest sense of the word, into a suitable and practically-applicable economic model. Clearly safety is not usually enough of a selling point (or unique selling point), and is even less persuasive when it means putting up the price of a product.

Nevertheless this analysis is based on faulty logic, based on a social misunderstanding: consumers do not refuse to pay the price of security, but consider to have already paid for the product or service and thus fully expect it to function as it should, without malfunctioning, without latent defects and without hidden functions. It wouldn't be logical for a manufacturer of tinned foodstuffs, having agreed a price with the client, to then present them with a second invoice for certification that these same goods were suitable for consumption. It is not that the security market shows poor accounting practices, but that security is just one of a mass of competing commercial requirements and products, making it difficult to isolate.

When considering a future economic model it is worth bearing in mind that the current one is weakened by this uncertainty as to whether security and service are already included in the purchase price. Moreover, the current consumer trend towards open source or free software indicates that consumers already consider software to be expensive enough, even with the supposed inclusion of security. The suggestion that consumers should pay more for security could only boost this trend.

Inversely, making this security visible and manifest to the consumer would add value to the software industry: with users having been left disappointed by promises which were not kept, this economic sector is showing falling customer numbers. In short, users feel they have already paid for security and over the next few years they are likely to spurn further purchases if, for the same price, they do not ultimately get this security (in its widest sense) in a way which is visible, manifest and verifiable by them (or by a trusted third party), or even partially configurable on request and to suit their own requirements.

If security can add some commercial value, it will be less in the hope of increasing software prices or sales but more to avoid the gradual exodus of disappointed consumers. With this issue, there are two vital criteria:

- The first, as previously mentioned, is visibility;
- The second is verifiability: something must be done so that customers and users can verify for themselves the functions offered and the way in which their personal data is used. Lest we forget, we are talking about rights already covered by various laws, as citizens often have the right to access or change data held on them. Without necessarily having to verify the source code, users could ensure that software running on their computers is doing what it is supposed to do, and nothing else.

Verifiability (and even the possibility of configuring certain functions) also relates back to those aforementioned ideas of minimum trust thresholds.

1.13.2 Ambiguous aims: to care or to cure?

Once the framework is in place, the debate can focus on determining whether the aim of the economic model will be to care or to cure. However we should not be fooled by the apparent simplicity of the caring/curing dichotomy:

- Are we to rely on incentives or penalties? It seems likely that a mixture of both will be necessary, but we need to define both proportion and content.
- Do we want a system which (whether it provides incentives or penalties) acts before or after the facts: the idea that there is an automatic link between incentives and prevention is often false, as exemplified by the additional insurance premiums (whether as an incentive or deterrent) which businesses or individuals must pay, *a posteriori*, for previously-committed errors. Inversely, repressive measures can often be implemented before the facts, as exemplified by speeding fines, which are imposed before an accident has occurred but which indicate how strong a possibility it is.

This point leads us to another unavoidable question: do we want to tackle errors and dangers which have already actually occurred; or rather, do we want to focus on high-risk behaviours? In the case of the latter, it is not that a matter of accident-prevention, but of acknowledging that an individual or economic entity put itself in a position to have caused an accident, regardless of whether it actually happened: should we then penalise the running of risks, or wait until the risk becomes an accident?

Are we therefore looking at curing bad behaviour or its consequences? Often, it is a matter of striking the right balance between the two.

1.13.3 Economic players linked to various economic models.

We need to look at what kinds of parties will be judging or arbitrating in these situations. There are a number of broad schools of thought on this issue: the law (which sets down limits or rules), the market, historical cost accounting etc.

1.13.3.1 The market

The market can be divided into various subsections:

These can take the form of quotation or securitisation of risk. These mechanisms have recently come under the media spotlight due to the recent financial and banking fallout. More generally, there is a particular contradiction in the case of ICTs, for which one of the desired criteria is transparency in being able to judge how secure or harmless retail products are. Pure economic theories currently suggest, amongst the basics of a liberal economy, that there should be transparency of products, players, and supply and demand mechanisms (and its corollary, the absence of any disparity in information between economic players) before any rating can be made. There would be a serious contradiction in demanding that a market list degrees of transparency, although this same transparency, at a more general level, is necessary to the accuracy of the assessment on which this quotation is determined. This leads back to the need for a result which, a priori, has its own source and method.

Can the market alone provide the basis for an economic model which includes security, privacy, transparency, etc?

If so, how do we restore the transparency required for it then to be judged itself? The principle of ratings agencies has recently been subject to criticism, which, without rendering the concept null and void, weakens the argument for it in an unregulated form.

Does perfect competition currently exist?

It is worth noting another important weakness here: economic theory stipulates that a market is only perfect under certain conditions (we have already seen the indispensable criteria for transparency and the absence of any disparity in information). These conditions provide a total competition situation, which itself refers to the atomicity of supply and demand, the absence of any barrier to entry or exit of the market.

The software market does not currently enjoy such conditions. Lest we forget, European authorities have taken up several emblematic cases, with legal proceedings and record fines. It would make little sense to rely on consumer reactions in the face of a lack of service provider security, if their ability to change is limited by commercial or contractual motives, or by a lack of individual technological skills.

The same goes for their ability to judge security levels, something which is not appreciable by the uninitiated.

There is a second branch of this area of the market which relies on insurance industry techniques, which are already used to gauge risks and to spread the cost of them out amongst the insured parties either a priori or *a posteriori* based on the possibility of a risk occurring or its actual occurrence.

- The anticipatory system is based on insurance premiums calculated on the basis of risks incurred, attitude, and the means and mechanisms available.
- Bonus/surcharge systems, in addition to the basic anticipatory system, also include *a posteriori* measures, which distributes the cost of insecurity (or for ICTs also a lack of privacy) based on observations of facts and individuals.

It is worth noting that the French authorities are currently looking to promote this bonus-surcharge system, and to extend the list of eligible products. This covers environmentally-rated products but such practices could also work in terms of ICT hardware and software security policies.

This initiative is being promoted as part of a "true environmental cost" initiative, which aims to encourage manufacturers to develop energy-efficient models with low consumption of raw materials and resources. These approaches are completely or partially transferable to criteria such as security.

Could a good economic model be created based on the insurance system, incorporating security, accountability, privacy and transparency?

The insurance industry, with its system of trust and visibility guarantees would also offer some useful reference points with regard to interlocutors who do not have the time or skill to make detailed checks on other interlocutors or systems. This domain would, then, work along the same lines as the existing accreditation and certification system.

1.13.3.2 The law

The law can be seen as an integral part of an economic model, as the various parties involved include in their potential expenses the cost of such items as fines for copyright infringement, convictions for offences, or even the cost of loss of freedom (those involved in computer piracy do measure, at least unconsciously, the profitability of a financially-motivated act by balancing it against the probability of spending a number of months in prison, counted as a liability.

Proposals have been made to consider various forms taxing the lack of security and personal data protection (in relation to the minimum required levels of data to be collected), etc. This approach could be either unilateral (a financial penalty for poor products, thereby generating additional charges compared to good products, and conferring to the latter a price advantage), or bilateral (taxing the lack of security, but redirecting money raised from such charges to those who have made efforts in this area).

This latter approach is partially compatible with the insurance company notion of bonuses/surcharges, in which the aim is not for individuals to support their competitors' injurious acts, but on the contrary to confer an advantage on those who adopt good practices. Here a choice has to be made as to whether we want these systems of either penalty or reward (through cross-compensation) to be governed by the law, the market or even by an insurance industry-type system. And moreover, to what extent public and private bodies will play a role in this.

1.13.3.3 Accounting costs

As reputation can be seen as a constituent part of individual or corporate capital, it can also be considered as a part of an economic model, as a company can judge the negative impact of adverse publicity over the intrinsic qualities of any of its products. This approach would therefore support the emergence of systems which disseminate information on known malfunctions and the risks inherent in certain software and hardware products.

There are then two questions to be asked: by what technological means is this information to be disseminated (which media) and by whom? The how and who could be based on spontaneous initiatives, co-operative movements, word-of-mouth/viral internet transmission, etc. There could also be public bodies, such as product ratings agencies, along the same lines as current electronic goods efficiency ratings (for electrical, water efficiency consumption, etc.). A similar type of authority also rates vehicle pollution emissions.

Accordingly, one of the major weaknesses of the present system is that consumers do not have enough information on exactly how safe currently-available products are and what potential

dangers they may pose. This lack of information stems from an almost identical problem on the part of the authorities.

It is worth pointing out that information can be collective (in which anyone can find out about the qualities and weaknesses of any product or interlocutor), as well as individual: the digitisation of communications paves the way to a ratings agency dealing with data flows, e.g. in the form of data flow authentication stamping readable by the recipient. This already exists in antivirus systems, which use a system of icons or pop-up boxes to indicate their status rating for a particular message or attachment.

2 Security and Trust Challenges

This section sets out the main Security and Trust Challenges for the security design of the Future Internet. A series of key security problems and issues that form the background to the research priorities, are discussed

2.1 Background

2.1.1 Two key structural vectors

The issues addressed include Security and Dependability challenges for the design of architectures, protocols and environments that will constitute future large-scale and globally networked ICT systems. Specifically, these focus on the upcoming future internet; cloud computing; the "Internet of things" (IoT) with mixed mode environments consisting of diverse computing, communication & storage elements; and, global e-Service infrastructures. The desired characteristics of dynamic, adaptive, scale-free, autonomic control are attractive in abstraction, though as global scale systems develop, heterogeneity (in design, resource types, operational policies, etc.) is often the pragmatic key attribute making systematic end-to-end security a challenge.

When considering the future research challenges and orientations, we need to take cognisance of the direction of these two dynamic vectors in the coming years:

1. **Ambient security continuum** : security technology will be everywhere, at all scales, in all layers, in the infrastructures, in the networks, the servers, the services, the content, the physical objects or in any sort of temporary virtual constructs (virtual private networks, dynamic software service coalitions, virtualised communication, computing or storage resources):
    a. Architecture and protocols: security is everywhere, spread throughout organizations, administrative domains or even national borders, particularly with governance of secrets and identity management;
    b. Core network: crypto at 1 Terabit/s, robust protocols between Autonomous Systems;
    c. Edge networks (3G++ but also IoT): decentralized, heterogeneous domains, and numerous scarce resources, where cryptography is difficult to implement;
    d. Content and services: multimedia downloading, distribution control, proof of ownership, illicit computations; insecure composite services and mash-ups;
    e. Critical infrastructures: resilience is everywhere. In particular there is a need to deploy critical infrastructures that can reconfigure and deliver under severe attacks, damages or human errors;

2. **Proactive security paradigms**: security paradigm evolution is essential if we want to move with the paradigm evolution of IT (virtualization, massive content, multiparty exchanges within social networks or within business value chains). This will require:
    a. Innovative security and trust models which better fit to the actual IT situation:
        i. Security and trust in the design of communication (other than store & forward) and cooperation (Web2, P2P, Internet of Things);
        ii. Security (stochastic), trust (reputation, recommendation, frequentation);
        iii. Contextual privacy with pervasiveness and location.
    b. Security and trust metrics to avoid qualitative biased judgments:
        i. Measurable variables for benchmarking, quantifying security validation (before and in operation);
        ii. Composition and meaningful aggregation of variables at all scales, in all layers, for assessing security status and enabling informed decision making.

c. Approaches to secure or protect the new representation and configuration of software, services and content.

2.1.2 Security needs

The future needs are:

1. Support for better identification, and accountability:
    a. must handle layers/domains: could be based on virtualisation;
    b. need policy-awareness as an architectural property;
    c. need observability as an architectural property;
2. Support for security monitoring:
    a. logging, log access, traceability;
    b. providing incentives for security data sharing: typical traffic mixes, current traffic snapshots, virus and worm signatures, typical attack signatures;
    c. fostering collaborative "environmental situation" establishment, collaborative anomaly detection and classification. States could create trustworthy, closed platforms for such practices.
3. Support for dynamic, contextualised trust:
    a. implies dynamic, contextualised policies;
    b. need tools/models for trust assessment and verification;
    c. need to support the full lifecycle;
4. "Everyware" security
    a. anywhere with transcontinental applications (compute here, store over there, access there)
    b. anytime with contracts
    c. anyhow with multi-models (societal, business).

2.1.3 Security principles

In order to solve these problems, and to overcome some contradictory or conflicting issues, we need to put forward:

1. A fair balance between transparency / visibility versus obscurity / opaqueness:
    a. Security is the art of sharing secrets within entities/components of a system;
        i. Privacy implies a shadow area for freedom;
        ii. Production secret to protect authors and creators (IPR, DRM);
    b. Trust is the art of sharing -any kind of things- ,including secret and sensitive, and of cooperating, in a relationship of two entities;
    c. Traceability requires observability with rules;
        i. Data gathering, recording, auditing;
    d. Governance requires knowledge;
        i. Governing means an ability to forecast (models derived from experience);
2. A new security and trust architectural approach : clean-slate versus incremental modifications for security:
    a. Moving target, moving methodology;
        i. New and emerging generations of attackers every three years (on a continual basis);
        ii. Future requirements from diverse users and society: unexpected usage;
        iii. Evolving future fundamental technologies.

2.2 Segmentations of the FI components

2.2.1 Network infrastructure

Core network

Characterised by:	Immense size but low density, one single authority, globally few actors;
Societal needs:	High reliability, climate meteorology, public situation awareness;
Technical needs:	Integrity, management, control, observability, big-big cooperation between different core networks (i.e. their authorities), internetworking;
Issues:	Data sharing, trustworthy situation, contract verification

Access network

Characterised by:	Huge and dense, one single authority per AN, dependence on core-network services, heterogeneity of technologies;
Societal needs:	Sufficient reliability, ubiquity of several ANs everywhere, transparent and fair AN selection: transparent, trustworthy criteria, discovery, service pricing; same service despite technological heterogeneity;
Technical needs:	Secure signalling and security signalling;
Issues:	Trust propagation (from home network to the Visited AN) and establishment (serving a nomad), heterogeneous security: policies, choices, cross-layer security enforcement

Edge compounds

Characterised by:	multi-authority (private-private, private-public, small-big, small-small, myriads of small, swarms, etc.), multi-technology constructs, relatively small but may include myriads of nodes;
Societal needs:	Easy to use, reasonably reliable and moderately secure;
Technical needs:	Access control to data and services, control of the whole: easy network on/off, controlled data sharing; controlled extension, additions, removals; robustness through redundancy and rerouting, adaptive, capability-aware security.
Issues:	Capacity of nodes, pairing, limited energy.

2.2.2 Services using or relying on network infrastructures

Critical Infrastructures

Characterised by:	Of public security and safety concern. Usually use telecom systems for control, observation, etc. I.e. private edge is controlled from a private platform of the same authority. In between we can have a typical telecom construct of different ANs and CNs.
Societal needs:	High robustness; no failures in whatever conditions; only controlled, announced turndowns
Technical needs:	System of system state and health establishment, trustworthy platforms for data/state exchange of stakeholders, propagation avoidance, usage/deployment of new operational models from security for security research.
Issues:	Availability.

Services

Characterised by:	Multi-party, at least two authorities (producer, consumer), implicitly running over a complex telecom infrastructure (may be a 3rd authority). Service architecture is another, different complex system.
Societal needs:	Fairness and integrity: announced readable clear pricing and correct billing, proof of involvement.
Technical needs:	Efficient secure service architectures, self-properties for lower operation cost for service providers, service composition for outsourcing/mutualisation of reliable components, provider-consumer-provider, etc. multi-party services, non repudiation, logging, accounting, traces.
Issues:	Reliable, secure remote execution and procedure invocation; control of exchanged data, in operation and post-operational (DRM).

2.2.3 Advanced Security Engineering

Further research on adaptive, programmable and extensible policies;

Further research on new operational models (survival, disinformation, deterrence);

Meterology and situation awareness: security data sharing, emergency centres;

Security observation, management, evaluation and validation (metrics);

Crypto research: new hash functions, multi-party operations, Tera-bps cryptography and authentication, biometric integration;

Issues: testing, comparison, validation of new proposed approaches.

2.3 Security of the future global digital ecosystem

2.3.1 Trustworthy polymorphic Future Internet

The focus is on building robust large-scale networked digital infrastructures and systems and on their secure interconnectivity (=> resilience, identity and accountability issues), guaranteeing massive audio-video traffic at very high data rates (=> traceability, identity, signatures, IPR issues).

Europe should become one digital plate of this dynamic, competitive plate architectonics, connected through “digital hubs”. It is important to clarify the promises and constraints to the citizens, but also to clearly express our requirements on and guarantees from the external partners.

2.3.1.1 Security of the core network and the critical nodes

1. **New protocols and architectures**: security at a very large scale, improvement of Internet peering systems and advanced Border Gateway Protocols between Autonomous Systems within the current Internet, reparcelling and providing robustness of the current mosaic of the Internet, probably through virtualization of Autonomous Systems.;.
    a. **Cryptography**: packet encryption at 100 Gigabit/s, flow authentication at 1 Terabit/s;
    b. New high data rate virtual routers with embedded **security by design**.
    c. Globally running applications and services (international VPN, grids, clouds, search engines) with **multi-legislation** issues: responsibility, traceability in an international environment;
2. **Security of the virtual paradigms** at all the layers and levels of the network: packets, channels, routing, bandwidths, sessions, networks, autonomous systems, operators, etc;
3. **New security architectures** to secure **high capacity storage server farms** and fast retrieval with huge data traffic in the context of the evolution of Internet with concentration

of critical nodes (Global Internet eXchange, server farms, high performance parallel computers, Web accelerators, Content Delivery Networks);

4. Regional **emergency control infrastructures** (very large scale: - country, Europe) to protect critical infrastructure and critical applications (financial networks, air traffic control), systems of systems (to avoid knock-on domino effects). This may include "infrastructural meteorology" services for infrastructures relevant to public safety and security. States should require publication of "climate" and "health" data and share it over a stock-exchange-like platform. Certain information might/should become mandatory, while other information might be optional or of a commercial nature. Control infrastructures: networked physical security balancing security and privacy, keeping individual privacy;
5. **Test beds and experimental facilities** for security of the Future Internet at the core level.

2.3.1.2 Security of the edge networks

1. **Federated security**: integration of heterogeneous security policies throughout several smart ecosystems;
    a. federation and coexistence of several conflicting security frameworks, in terms of identity and levels of security assurance;
    b. security or trust models are needed for negotiating compatibility or interoperability in an open or fragmented environment;
2. **Seamless security**: Interoperability of security schemes throughout the heterogeneous landscape of access networks (3G++, Ad hoc, Sensor, etc)
3. **Transparent and user-friendly security**: security improvement of wireless technology such as:
    a. mobile phone as multi-media device;
    b. virtual desktops with enterprise data and software;
    c. mobile/wireless communications across heterogeneous infrastructures in various mode, opening and interconnection of different infrastructures and nodes;
    d. distribution control of private and/or enterprise data: data deployment, concealment and removal from various wireless devices.

2.3.1.3 Multi-polar governance and security policies between a large number of participating & competitive stakeholders

1. **Mutual recognition security frameworks** for competing operators: Telecom Operators, Network providers, Service/content providers; sharing security secrets: improvement, or replacement of PKI-like security infrastructures, improvement or even replacement of DNS and ONS; collaborative and shared security mechanisms;
2. **Transparent security** for re-balancing of the unfair, unequal face-to-face relationship of the end-user in front of the network: governance of the infospheres of people => scalability, traceability, log data management, accountability management.
3. **Instruments** for **early detection of attacks**: new methods to filter adware, spam and eradicate malware and viruses (included on 3G++ smart-phones), tools and mechanisms for large-scale test-beds dedicated to security (attack simulators);
4. Real time and **large scale tests for crisis management** procedures.

2.3.2 Trustworthy global computing

The development of the ICT systems is characterized through change towards more openness, more complexity and, most importantly, through the reinforcement of links to the real, physical world (communicating objects, intelligent environments, networked control systems in home automation, aviation, car industry, power grids, medicine and healthcare, etc). The ICT technology is no longer in a distinct closed virtual world.

The focus is on building confident services to avoid misuse, to detect failures, and to sustain the quality of these services. The composition, orchestration of these services requires secure mechanisms for dynamic configuration of these components.

Users need, by default, to give the minimum identity attributes to access to these services and content. The security requirements need to be analysed through a business risk approach: identification of subjects, encryption of protocols, secure base software and middleware, tamper-proof applications are among the important features for securing services.

Europe should lead the technology integration for the use of available, dependable, secure services onto the networks.

2.3.2.1 Security of the cloud computing

The focus is on security of future smart Web, social networks, cloud computing, grids, P2P, large distributed environments, generalized virtual networks (=> privacy and trust issues).

1. Security of the new Web services and privacy protection against observability or linkability through search engines or social networks, etc.
2. Collaborative environments, cloud computing :
    a. compartmentalization of the clouds or security of virtual entities;
    b. virtual spaces are ways to cooperate with real objects, to represent knowledge (Web2 technology, multimedia), immersive spaces are new approaches for simulation of the real world;
    c. sharing resources (computation, storage, exchanges) in a secure manner.
3. Automatic maintenance of the new digital scenes:
    a. long term and constant housecleaning of the personal infospheres;
    b. right to oblivion.

2.3.2.2 Domai-specific trust, security and privacy for smart environments

The focus is on contextual security with secure smart services for sharing information and cooperative environments with societal acceptance in order to feel in control of the digital ambience, and on new infrastructures using ICT as a tool to make the real world artefacts more reliable.

1. e-Health: secure online checking, resilience in telemedicine, security at the hospital, privacy of patient medical record databases, resilient smart assisted digital living (usability and acceptability issues), medical implants (resilience);
2. e-Home: urbanization of the intelligent home, remote assistance (access control issues), privacy and personal integrity issues (ageing population, ambient assisted living);
3. e-Government: electronic voting at large scale, law enforcement database with individual data (privacy issues);
4. u-enterprise (ubiquitous enterprise, virtual desktop), e-Transport, e-education, e-Commerce, u-service (discovery, location privacy);
5. Internet of Things (RFIDs, NFC) : security infrastructures incarnated for niches (logistics, plants, medical, library);
6. immersive environment, entertainment: 3D Internet, video games, massive multiparty networked games, virtual casinos (auditability issues);
7. control and automation systems.

2.3.2.3 Resilient, pervasive, self-organised computing

Self-* networks will have to move on from the obsolete concept of end to end connectivity and embrace situations in which nodes are devices which cooperate freely and spontaneously in the absence of centralized 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.

The focus is on security of wireless sensor systems, pervasive networking, opportunistic networks, and mobility systems, self-organized infrastructures, dynamic heterogeneous distributed environments (=> dependability, integrity and privacy issues).

The common issue here is security in presence of scarce resources

1. Security for self organised, and other self* like ubiquitous computing systems (reconfiguration, management and repair) taking into account personal integrity, system autonomy (robustness, management), adaptive security, and machine learning of security models;
2. Security of sensor networks
    a. Adaptive security: do not try zero or full security; better provide some security than nothing (protection with scarce resources). Would need new, respective policies and adaptive and situation-aware implementations/mechanisms. Typical application: Energy-aware security. Example: only authenticate a fraction of nodes and not all nodes in the path. Switch off encryption when low on power. Other possibilities include: design with heterogeneous nodes, some nodes may not be able of certain operations, adapt service security as far as the policy allows that to be able to communicate with these nodes.
    b. Security and aggregation: in sensor networks, data aggregation is an essential paradigm. Data aggregation, when combined with the respective verifications, can be used to provide some structural security of sensor networks.

2.3.2.4 Security of services and content, of software and data

Future services will be based on the notion of context and on knowledge. They will have to cope with highly dynamic environments and changing resources, and will have to evolve towards more implicit and more proactive interaction with humans. Content providers will play a decisive role in this context.

The technical paradigm shift leads from protection/prevention (cryptography, access control, confidentiality through pre-established policies and respective security associations) to other operational security models.

The goal is to build components, products, services and systems with an acceptable and affordable assurance of trustworthiness.

1. **Security of services**:
    a. security policy compatible with business models;
    b. secure software lifecycle management (particularly security of software upgrades);
    c. security of increasingly dynamic aggregation or composition of services;
    d. security of middleware, distributed grids, peer-to-peer exchanges, collaborative work platforms, distributed applications involving a large number of simultaneous users.
2. **Protection of content** and **Intellectual Properties**:
    a. managing and controlling the **life cycle of personal entities** (whether data, programmes or traces) and dealing with related security issues.
    b. IPR service infrastructures, for content sharing, media distribution; protection and management of IPRs; security of audio video contents; fine-grained access to documents and usage control of distributed data;
    c. dissemination of private data to a public platform without loss of control and ownership (does not necessarily imply IRP/DRM), access control can be done through cryptography and complex key management;
3. **Usability** and security: hassle-free security, user security they can understand and privacy they can control.

2.4 Trust and Privacy when interacting with digital entities

Let us not forget that the future of ICT raises human and social issues. What type of digital systems should we consider for daily lives that are compatible with our values; how should we view the relationship between knowledge and the capacity of physical persons and their cultural and emotional requirements? What are, what will be and what should be the social implications of the

development, deployment and use of such systems? The evaluation of technology on a precautionary basis should guide the design of tools for the construction of ICT, ultimately not purely driven by the evolution of technology, but with a basic objective of improving the quality of life.

Pillars of privacy and trust are not just technology but education, law, governance (feedback cycle: measuring / enforcing), safety Net.

2.4.1 Identity management

There seems to be a broad consensus on the desire for flexible identity systems. This could take two possible forms. Citizens could have an "à la carte" choice regarding the sending and receipt of data streams:

- The ability to decide on the level of security of data streams concerning them (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.

Following the accountancy model, based on a reliable identity, to be attached to an initial territory-based registration, it would be possible to temporarily abandon this reliable identity for a particular data stream or connection, but without being able to divest oneself of the rights or facilities which the recipients or operators might require from these same streams attachable to a trusted identity.

We need to design and deploy a collection of Identity Management frameworks in order to identify through distributed infrastructures, end-users, services, contents in different situations.

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 all networks, and such that reliable and more or less exhaustive incoming and outgoing accounts can be drawn up.
- Reintroduce, on a lower network layer, a "territorialisation" of facts and participating parties. The aim being 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.

Other approaches have been suggested, and are worth looking at in greater detail; however, the two principal options mentioned above seem to have immediate unifying and organisational potential.

This two-pronged global accountancy and re-territorialisation approach could offer an alternative to the mutually opposing laisser-faire/network policing options. It could also buck the network trends towards ubiquitous practices, nomadism and varying identities.

1. Identity management, accountability, traceability frameworks:
    a. at the network level:
        i. to balance privacy and traceability and prevent cyber-crime and frauds
        ii. Secure management (at large) of the different network entities;
        iii. Remark: several frameworks may coexist; protocols to interact with foreign frameworks are an open issue.
    b. at the service level:
        i. with pseudonymity, while keeping large anonymity;
2. Interoperable framework throughout European Member States of Identification and Authentication

a. with multiple authentication devices, e.g. identity and authentication of ontology, virtual identities (Trusted Platform Module for hardware, smart cards for persons), biometry at large. (using multimodality: biometry, RFIDs, NFCs, physical objects, etc);
b. taking into account diversity of services (governmental, financial, medical) and richness of cultures;
c. management of profiles and identity attributes, keeping privacy, while improving searching and indexing relevance;
d. deployment of new digital signatures : cryptography of new schemes for digital signatures (to overcome the current hash function attacks - See the NIST International competition for new hash functions and new digital signatures.);
e. auditing and reporting, access and authorization control.

3. Profiling services and communities
    a. Trust and privacy issues need to be addressed for the relationship between user and services, communities of users and categories of services.

2.4.2 Trust infrastructures

Lack of trust is one of the main barriers to the establishment of a secure and dependable Information Society. This can be a lack of trust in the cyber-infrastructure, due to frequent attacks or fears about the design of digital systems. It is also caused by concerns about privacy, as well as by the difficulty in modelling trust relationships among digital entities and between humans and digital entities. The panel focussed on key elements necessary for securing the applications and services operating across future large-scale networked systems, including trust management models and the articulation of security and privacy to reinforce trust, with emphasis on user-centric privacy enhancing technologies, mechanisms for accountability, liability, and monitoring, and a privacy-respecting naming and identity-management framework (of individuals, organisations and digital entities).

The absence of a measurement of trust in digital systems is one of the major obstacles in the maintenance of networks and telecoms infrastructures in a controlled state, both in terms of security and reliability of operation.

The lack of trust in ICT infrastructures shows itself at every stage in their life cycle: during operation, because these systems have to confront intentional attacks or cope with accidental breakdowns and at the design stage because security or robustness are often not included in the system's specifications.

1. **Trust infrastructures** (Public and/or Private Trust Infrastructures): instrumentation of the network periphery provided by trusted new stakeholders, computing trust and security assurance, using diverse trust models (by reputation, by recommendation, by frequentation, by voting). Trustworthy providers may coexist for various services, with different levels of confidence (governmental, business-wise for-commerce, etc);
    a. Trust architectures and new protocols to delegate trust and partial trust;
    b. Trust infrastructures in a dynamic business environment with newcomers, insiders and outsiders, ingoing and outgoing stakeholders: emergence of new stakeholders: process, methodology and certification or homologation procedure to validate and check services (a priori, a posteriori);
2. **Trust instrumentation** at the end-user level: using the user as trust sensor, but also giving trust-relevant feedback to the user at the service interface;
3. **Cognitive** and learning **instrumentation** for trust:
    a. Due to sophistication of technology, integration of abstract components, co-ordination of services, autonomic tools are needed to increase confidence in the complexity management for the societal acceptance.

2.4.3 Privacy infrastructures and mechanisms

Logged by operators or providers who run digital systems and picked up by sophisticated sensors in monitoring systems, the digital trail left by everyone, wherever they go, can go to make up far more detailed data files than the traditional files compiled by bureaucratic administrations.

With these techniques we reach a whole new level and individuals can no longer keep in their own possession information about them which they do not wish others to see. Surveillance and GPS tracking techniques pose formidable problems when it comes to protecting personal privacy.

Objectively verifiable data was previously compiled and managed with specific and known purposes in mind. Now, however, the data-gathering system operates 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.

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.

1. **Privacy infrastructures**: protocols, tools to check privacy assurance, and multi-identity systems keeping privacy;
    a. Sandbox security models to improve privacy issues;
    b. Right-to-oblivion security models, networked garbage collector instruments to clean personal data across infrastructures;
2. **Privacy of personal** sensitive communicating **devices**: massive deployment of intelligent devices (3G terminals, PocketPC, PC) and growth of sensitive personal data
    a. Personal trusted entities (next generation smart cards, …)
    b. Wearable and/or transportable embedded systems,
3. **Privacy & Traceability** of personal **behaviour**:
    a. Unobservability (controlling unwittingly tracings), unlinkability while supporting user's profiling and tracking to enable personalised services;
    b. Usability with diversity (diversity in Europe);
    c. Ethical issues;
        i. Illicit content, illicit computations, legal proof, content control & filtering;
        ii. Security in obscurity : we must not be hostage of one security mechanism: security Sensors manageable by end-users to "measure security assurance";
4. Digital Sovereignty
    a. Audit, proof of the past;
        i. Authentic memory of an Information system;
        ii. Auditability of personal databases;
    b. Access control & filtering;
        i. Security of content (IPR, DRM…);
        ii. Filtering of virus, unsolicited contacts & messages (spam, spit, spim), bots.

2.5 Measurements, metrics, models, methodologies and tools (M4T) for security, dependability, trust and privacy (SDTP)

2.5.1 M4T for ever-increasing complexity

1. Security for the composition of systems, security of systems of systems: more abstraction in the security paradigms (security of virtual systems, entities, etc);
2. Security of a pervasive environment with scarce resources: using statistical approaches, lightweight security models;
3. Circumvention security models, survival systems (to avoid the current routines of patching of patches);

2.5.2 M4T for quantitative security assessment and predictive security

1. Consistent measurements and data collection at a large scale to manage complexity, to measure availability and maximum downtime, to feed trust models, to configure in real time protection devices, etc, while achieving balance of privacy and security (statistical effective data collection, anonymisation of personal data);
2. Trust and Security models, tools and principles
    a. For adapted to local cultures : behavioural and mobility models for simulation and prediction to feed simulation models with relevant parameters;
    b. to specify the behaviour in higher abstractions and verify through formalisms (theorem proving, model checking, etc) in operations.
    c. to build large scale systems for crucial societal applications, taking into account:
        i. composition: if basic elements (primitives, elementary devices, etc) are reliable, trustworthy and secure, how can we guarantee that their composition to a more complex structure inherit these properties?
        ii. evaluation (metrics) to evaluate the correctness, quality, efficiency, reliability and, finally, security of security, especially, in a working operational setup, during execution.

2.5.3 Enabling technologies and standardization

1. Declarative languages in security: metadata, ontologies.
2. Multimodal biometry, secure OS for smart phones, TPM environment, new cryptography (elliptic curves);
3. Standards in security to make tools and instruments interoperable or compatible.
4. Certification and measuring level of confidence.

2.6 Disruptive security

The only way to make a significant leap to improve security and trust within the digital world and to make it more reliable is to introduce new security models and to implement them with new languages which include security concepts within their semantics.

These new models and languages for trustworthiness could be used in three disruptive contexts: green security, just-in-time security, polycentric security.

Finally, we must not neglect the possible arrival of Quantum technologies with new threats (cracking current asymmetrical cryptography) but new opportunities (new models to assess security and trust). We need to think about classical cryptography in the quantum era.

2.6.1 Green security

The focus is to save resources (energy, CO2), and to think in terms of sustainability and in terms of global energy management.

1. Security heuristics at the network level to prevent propagation of epidemics;
2. Metering security personal tools.
3. Integration security approaches to optimise and to share security resources, detecting maximum anomalous event at the source level, and inserting minimum security algorithms within the end-user terminal.

2.6.2 Just-in-time and real life instantaneous security

The focus is on protecting volatile digital life in vivo (*hic et nunc*), in real time (=> privacy and trust issues).

1. Tools and models for nomadism: real-life end-user security, instant or just-in-time security protocols, real time security in crisis situations; trusted secure tokens & devices (sensitive devices); secure, multiparty, massive videogames;

=> Raising automatic security tools dealing with overflow of events;

2. Delegation security to nomadic personal robots, swarms of objects, body area networks (medicine);

   => Trust infrastructures to ensure and speed up the interactions with ambient intelligence.

2.6.3 Polycentric security

1. Vernacular Internet: polymorphous security models, multi-polar governance: (=> scalability issues in the multi-facets management);
2. Spatial and geographic security: security with landmarks, new cryptographic protocols using trustworthy geo-reference systems (hour and location) (=> intermediation issues).
3. Multidimensional integrated security: derivation of high level security policy with fusion of multimodal securities from different sources to influence knowledge and trust and to upgrade user's awareness.

2.6.4 Quantum Networks

Quantum Computers should appear around 2018. We need to continue the European effort to support the development of quantum technology through the deployment of high secure services with quantum communications.

Quantum Crypto may achieve high secure distribution of secrets that classical cryptography cannot - and Quantum Crypto will be used in the context of omnipresent security technology in the future.

3 Future Internet and Cloud: Trust and Security Research Priorities

There are several areas of Trust and Security which need to be addressed in order to move securely into the Future Internet and Cloud computing domains. In this respect, Think-Trust recommends focusing on the development of a robust research agenda. In this section of the document, four major areas of Research Priorities are discussed. These will be updated and further developed for the final version of this report.

3.1 Security in (heterogeneous) networked, service and computing environments

The issues addressed include the elaboration of security challenges for the design of architectures, protocols and environments that will constitute future large-scale and globally networked ICT systems. Specifically, these include and focus on the upcoming future internet, cloud computing, the “Internet of things” with mixed mode environments consisting of diverse computing, communication & storage elements, and global e-Service infrastructures. The desired characteristics of dynamic, adaptive, scale-free, autonomic control are attractive in abstraction, though as global scale systems develop, heterogeneity (in design, resource types, operational policies, etc.) is often the pragmatic key attribute making systematic end-to-end security a challenge.

- Encompasses virtualization, cloud, private / semi-private spaces, realized by service "oriented" platforms
- Makes underlying infrastructure resilient in all environments and conditions
- Includes technologies to realize the ecosystems with key attributes of (mixed-mode) heterogeneity (of devices, device resource capabilities networks/connectivity, mobility, density and applications) and scale-less scope for growth
- Multi-domain security ad esp. across the interfaces (technological and user-level)
- Managing heterogeneous computing environments and corresponding trust domains
- Moving from physical security architectures to service level security architectures
- Need for conformal multi-domain security and especially across the interfaces (technological and user-level) where most of the problems arise

3.1.1 Trustworthy polymorphic future internet

3.1.1.1 Security of the core network and the critical nodes

- Protocols and architectures: security at a very large scale and a high data rate (embedded security by design), globally running applications and services with multi-legislation issues in an international environment; security of high capacity storage server farms and fast retrieval with huge data traffic;
- Critical infrastructure protection for critical applications, networked physical security balancing security and privacy.

3.1.1.2 Security of the edge networks

- **Federated** security: integration of heterogeneous environments throughout several smart ecosystems;
- **Seamless** security: interoperability of security schemes throughout the heterogeneous landscape of access networks (3G++, Ad hoc, Sensor, etc)
- **Transparent** and **user-friendly** wireless security.

3.1.2 Trustworthy global computing

3.1.2.1 Domain specific trust, security and privacy for smart environments

Contextual security with secure smart services for sharing information and cooperative environments with societal acceptance in order to feel in control of the digital ambience, and on new infrastructures using ICT as a tool to make the real world artefacts more reliable in e-Health, e-Home, e-Government, u-enterprise, e-Transport, e-education, e-Commerce, u-service, Internet of Things (RFIDs, NFC), immersive environment, 3D Internet, control and automation systems.

3.1.2.2 Security of the cloud computing

Security of future smart Web, social networks, cloud computing, grids, P2P, large distributed environments, collaborative environments, generalized virtual networks: automatic maintenance of the new digital scenes (long term and constant housecleaning of the personal infospheres), right to oblivion.

3.1.2.3 Resilient pervasive, self-organised, opportunistic computing

Security in presence of scarce resources:

- Security for self organised, and other self* like ubiquitous computing systems
- Security of sensor networks : adaptive security and data aggregation in sensor networks

3.1.2.4 Security of services and content, of software and data

Future services will be based on the notion of context and on knowledge. They will have to cope with highly dynamic environments and changing resources, and will have to evolve towards more implicit and more proactive interaction with humans. Content providers will play a decisive role in this context. The goal is to build components, products, services and systems with an acceptable and affordable assurance of trustworthiness.

- Security of services: security policy compatible with business models; secure software lifecycle management; security of increasingly dynamic aggregation or composition of services; security of middleware, distributed grids, peer-to-peer exchanges, collaborative work platforms, distributed applications involving a large number of simultaneous users.
- Protection of content and Intellectual Properties:
- Usability

3.2 Trust, Privacy and identity management (metasystems) infrastructures

3.2.1 Trust and Privacy Infrastructures

3.2.1.1 Trust

1. Trust infrastructures (Public and/or Private Trust Infrastructures): instrumentation of the network periphery provided by trusted new stakeholders, computing trust and security assurance, using diverse trust models (by reputation, by recommendation, by frequentation, by voting). Trustworthy providers may coexist for various services, with different levels of confidence (governmental, business-wise for-commerce, etc);
    b. Trust architectures and new protocols to delegate trust and partial trust;
    c. Trust infrastructures in a dynamic business environment with newcomers, insiders and outsiders, ingoing and outgoing stakeholders
2. Trust instrumentation at the end-user level: using the user as trust sensor, but also giving trust-relevant feedback to the user at the service interface;
3. Cognitive and learning instrumentation for trust:

    Due to sophistication of technology, integration of abstract components, co-ordination of services, autonomic tools are needed to increase confidence in the complexity management for the societal acceptance.

4. Profiling services and communities

   Trust and privacy issues need to be addressed for the relationship between user and services, communities of users and categories of services.

3.2.1.2 Privacy

1. Privacy infrastructures: protocols, tools to check privacy assurance, and multi-identity systems keeping privacy;
2. Privacy of personal sensitive communicating devices: massive deployment of intelligent devices (3G terminals, PocketPC, PC) and growth of sensitive personal data
3. Privacy & Traceability of personal behaviour:
   a. Unobservability (controlling unwittingly tracings), unlinkability through search engines or social networks while supporting user's profiling and tracking to enable personalised services;
   b. Usability with diversity (diversity in Europe);
   c. Ethical issues;
4. Multi-party security & privacy protection technologies.

3.2.2 Identity Management metasystems

Identity provision, choice and management: real and virtual, distributed & multi-layered, partial - ID's for users, systems, devices, services. Make existing and future identity management systems interplayable.

Quantification of S&P interplay + user-in-the-loop/user-in-control(?) S&P characterization.

- Identity management, accountability, traceability frameworks:
  - at the network level to balance privacy and traceability and prevent cyber-crime and frauds (Remark: several frameworks may coexist; protocols to interact with foreign frameworks are an open issue.)
  - at the service level with pseudonymity, while keeping large anonymity;
- Interoperable framework throughout European Member States of Identification and Authentication
  - with multiple authentication devices (using multimodality: biometry, RFIDs, NFCs, physical objects, etc);
  - taking into account diversity of services (governmental, financial, medical) and richness of cultures;
  - management of profiles and identity attributes, keeping privacy, while improving searching and indexing relevance;
  - auditing and reporting, access and authorization control.
- Standardization of effective and yet federated authorization frameworks

3.3 Underpinning engineering principles + transparency / accountability architectures + measuring

3.3.1 Engineering principles to establish trust, privacy and security

This covers

- Measuring trust, security & privacy for improving capabilities for engineering
- Establishing transparency, accountability and privacy properties for the main computing entities and domains
- Transparency, accountability and privacy / pseudonymity architectures

3.3.2 Metrics and tools for ever-increasing complexity, quantitative security assessment and predictive security

3.3.3 Measurements and data collection at a large scale to manage complexity

- to measure availability and maximum downtime, to feed trust models, to configure in real time protection devices, etc, while achieving balance of privacy and security.
- to build large scale systems for crucial societal applications, taking into account composition and evaluation (metrics).
  - composition of systems, systems of systems
  - pervasive environment with scarce resources
  - circumvention security models, survival systems
  - behavioural and mobility models

3.3.4 Enabling technologies and standardization

- Declarative languages in security: metadata, ontologies.
- Multimodal biometry, secure OS for smart phones, TPM environment, new cryptography (elliptic curves);
- Standards in security to make tools and instruments interoperable or compatible.
- Certification and measuring level of confidence.

3.3.5 Cryptography

- packet encryption at 100 Gigabit/s, flow authentication at 1 Terabit/s;
- deployment of new digital signatures : cryptography of new schemes for digital signatures (to overcome the current hash function attacks);

3.4 Data, Policy Governance and socio-economic aspects

The FI will provide a new volatile, massive and dynamic “urbanization” of data throughout clouds, networks, smart ecosystems. The status of these data, distributed all over the world, with multi-legislation will give to the data governance an important glue role, allowing a seamless but controlled way to deal with information.

3.4.1 Data and Information governance

Acquisition, dissemination, access, storage issues in the ubiquitous scale-less Web x/Cloud

3.4.2 Data management and liability issues

Security is desired to be technology invariant (not technology-agnostic).

3.4.3 Multi-polar governance and security policies between a large number of participating & competitive stakeholders

1. Mutual recognition security frameworks for competing operators: Telecom Operators, Network providers, Service/content providers; sharing security secrets: improvement, or replacement of PKI-like security infrastructures, improvement or even replacement of DNS and ONS; collaborative and shared security mechanisms;
2. Transparent security for re-balancing of the unfair, unequal face-to-face relationship of the end-user in front of the network: governance of the infospheres of people => scalability, traceability, log data management, accountability management. Security, trust & privacy policy management aspects: automatic policy enforcement, policy negotiation;

3. Instruments for early detection of attacks: new methods to filter adware, spam and eradicate malware and viruses (included on 3G++ smart-phones), tools and mechanisms for large-scale test-beds dedicated to security (attack simulators);
4. Real time and large scale tests for crisis management procedures.

3.4.4 Economical aspects

1. Business models
2. Security markets for identity management

Annex 1 Summary of Findings – WGs workshops #1 and #2

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

T-T Working Groups - Workshops 1 & 2: Summary of Findings

Issue: **Issue 1.0**

Date: **09-Jul-2009**

Editors: Keith Howker khowker@tssg.org
Jim Clarke jclarke@tssg.org
Brian Foley bfoley@tssg.org
Kieran Sullivan ksullivan@tssg.org

Preface

This report consolidates the main findings of the two Think-Trust Working Group workshops. Their main purpose was to look at where specific efforts are needed to deliver trust and security for the globally-interconnected digital information and communications infrastructure (sometimes referred to as cyberspace), and particularly for the Future Internet. This was mainly with respect to R&D, but the required "non-technical" dimensions of the environment, eg, the regulatory framework, awareness, personal aspects of usability, were also considered.

The workshops concentrated on a user-centred perspective: concentrating on the needs of the users themselves, their privacy and digital sovereignty and the services they use, but also remaining conscious of the defences needed for the underlying infrastructure.

The findings are in response to considerations of the range of problems from currently identifiable shortcomings to the challenges that anticipate future user requirements and the rapid developments in technology and usage:

(a) further or new research to develop technologies and potential solutions to the issues and challenges;

(b) adaptation and re-engineering, applying currently-available technologies;

(c) education & awareness
- for the user
- for industry (what needs to be done, and what possible incentives can be identified/provided)
- for policy makers (implications of new developments)

They are not presented here as detailed recommendations or worked-out statements of requirement for future R&D. Instead, in their totality, they can be used as evidence, back-up or reference for this purpose with some careful consideration.

Common Assumptions

There is broad acceptance that the current Internet and accessed services fail to provide the means to satisfy quite basic needs for trust, security, and resilience, and that something has to be done to fix the situation – *The status quo is no longer acceptable* [1].

Other than SSL, there is little to protect the ordinary user's information and identity whilst in transit, and no guaranteed protection once in the hands of a service provider other than the requirements of the Directives [2], which are frequently not met. Specialised users such as finance and government may have developed in-house and private network protection, but all Internet users appear vulnerable to certain attacks and accidental malfunction. With increasing global dependence for much social, economic, and administrative activity, the consequences could be catastrophic [3]

Some general characteristics of future digital environments are:

- that it will be a ubiquitous and pervasive, comprising multiple heterogeneous, polymorphous infrastructures and technologies that must interoperate and that will dynamically interconnect, (re)configure and compose;
- that user-centricity is a critical consideration and goal;
- that the current problems must be fixed, and that trust and security be taken fully into account for future developments;
- that we cannot predict longer-term what entities, protocols or business scenarios will be entailed in the Future Internet [4].

Summary

The main goal of the Think-Trust Working Group workshops has been to provide findings and recommendations for input to the RISPEPTIS [5] Advisory Board for its report, and to feed into the considerations and planning of future research in the Framework Programme. The first workshop took a general, open approach; the second focussed on four use cases, proposed by RISEPTIS, together with material from related sources including current projects, the FIA initiative, and ICT2008 sessions, etc. The use cases covered the trust and security needs for electronic identities, the challenges of joined-up eHealth services, Cloud computing, and the nomadic and mobile user. The common theme was to place the European user and citizen central to considerations, but also to look beyond, to the global context.

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

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

The second group centres on what is needed to support the nomadic, mobile user, and to enable the trusted use of Cloud-based services. A number of key characteristics and requirements are identified, together with an indication of possible regulatory support. These highlighted the need for a *standardized* architectural framework for trust and security, with the use of virtualisation to maintain separation between entities in an environment where physical boundaries have broken down. Within the architecture, a measurement infrastructure is needed, that can monitor security status and indicators, identifying and analysing attacks and intrusions, and building insight into merging threats. Continued development of underlying technologies is needed to keep pace with the demands of the growing size, complexity, capacity, speed, and heterogeneity of the networked digital environment. Accountability, that must be respectful of privacy, is seen as vital in ensuring transparency, deterring malicious action, and providing diagnosis of failure. Possibly also typical of other platform/service-related areas, a specific need for automated security policy governance was identified, extending from the formulation and agreement of what is to be provided with respect to aspects of trust, privacy and security, through the monitoring and reporting conformance of operations, and on to remedial actions for non-compliance.

1 WG1-related – Security, Dependability and Trust in the Future Internet

1.1 Architecture for Trust and Security

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

(a) provide for robustness of networks, network components, end-systems and –components to protect against intrusion and damage;

(b) protect the user, user information, and services.

Many topics below call for some sort of framework, mainly to support interoperability. These potential components need to be normalised and built in to a unifying, comprehensive Architecture.

Architectural issues

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

Architectural support must be provided for trust and privacy aspects of the Future Internet:

(a) first, with regard to transparency - security monitoring, observability and measurability and for data logging and log access;

(b) 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 (see below) 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.

1.2 Accountability

Accountability is fundamental to developing trust in ICT networks and services. All actions and transactions should be ultimately attributable to some user or agent (inc. as a special case Anon?). 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 where large amounts of data are being logged. There are also inherent privacy concerns surrounding the disclosure of such logs; 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 incorrect 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.

When establishing a means of redress by means of accountability/responsibility logs, a business-level model may be required. Lessons may 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. (note: see also policy governance, below)

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 require new work in technical standards together with possible regulatory support – an architecture/framework defining boundaries, domains, mechanisms, protocols, and processes to deliver comprehensive interoperability.

1.3 Virtualisation

As physical domains and frontiers dissolve and blur, new virtual separations and boundaries must still be established, and maintained in cyberspace. Virtualisation and the mapping of physical resources into virtual constructs will need to 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 understandable, manageable components.

1.4 Interoperability

A specific need for automated (security) policy governance was identified. This governance extends from the formulation, agreement, and establishment between parties 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 and redress for non-compliance. The arena for all this is again the generalised, mobile, polymorphic dynamic environment. The big challenge appears to be how to provide it without burdensome operational overhead and costs.

However, it appears that this may have common characteristics that are 'typical' of a number of basic functions, which are required to operate across a range of platforms, 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.)

1.5 Measurability, Metrics, Monitoring, and Reporting

Monitoring and measurement of events, actions, operations, etc. is necessary for an insight into security-related behaviour, both normal and abnormal. This allows the better provision of defences and responses for the benefit and improved protection of the network, the user, and services.

A broad understanding is required of metrics and what is to be measured, of the scope for a measurement and monitoring infrastructure, analysis of attack and failure, the economics (costs and benefits), and tools for incorporation into network systems and services that will contribute to their transparent behaviour.

Q: ultimately, is the only common unit <cost>
(rather than, say, <impact> = (*frequency* ∗ '*seriousness*')per *operation* per *user*)

Traffic and incident data relating to abnormal security events – intrusions, attacks – will support improved recognition and analysis, in turn leading to improved countermeasures (defence and response).

The gathering and sharing of data on attacks, intrusions, and system failures is understandably a sensitive issue to the victim. In addition to plain embarrassment (personal, .com and .gov contexts) such information may be of benefit to an adversary. However the sharing of such information is

vital to the improvement of defensive responses, planned recovery, and possible counterattack. The incentives to share has to overcome the reluctance; these may in extremis include regulatory reporting requirements if seen as part of a move towards a robust and resilient infrastructure that supports societal values, personal privacy and maintains a fair and open economic market-place. This will enable the establishment of trusted collaborative centres for data collection and response solutions.

Once again, some standardised framework is needed to allow controlled, trusted sharing and processing of information.

1.6 Protection of Network Resources

Although the findings of the Working Groups have been mainly in terms of the needs of the user, ultimately a dependable underlying infrastructure is critical to delivering the benefits from those areas.

Simplified goals include

- prevention of intrusion and penetration by accidental or malicious action;
- built-in robustness and recoverability for users, services, and the (communications) networks and their components;
- redesign, re-architect, and re-engineer as and as necessary, where this may have to include protected, privileged, channels for critical infrastructure, and even physical separation for emergency control and management of security and protection (see below).

The information and communications networks are largely owned and operated by the private sector. There are inevitably costs in providing the robust engineering needed, and public-private collaboration is likely required to ensure delivery.

The development of collaborative centres for incident reporting and collection, as 0 above, is vital to maintaining a vigilant and responsive defence against intrusion and attack – and accidental failure. International cooperation is essential in developing a coordinated response capability to major incident and threat, and again, public-private collaboration is needed to develop a comprehensive approach.

1.7 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.) alternatives;
- 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 (1): we need to weigh up the considerations of cost and economics, power and energy versus strength, performance and functionality;

- Basic engineering (2): control and management infrastructures separated from the normal user/service 'layers', cf <out-of-band-signalling>, possibly physically separate, higher-cost, hardened mil-spec connection and functional components, so not subject to common failure and attack (the converse of current sub-letting of some Critical Infrastructure to the public networks, however this is not to suggest that management control should share cyberspace with all CI)
- 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;
- technological vigilance – what is coming over the horizon, and what are the implications (eg, quantum technologies, nano-technologies, bio-(geno-)technologies, photonics, …)

2 WG2-related – Privacy and Trust in the Information Society

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

- Privacy: protection of all aspects of 'me'
  - Identity-related, location and time, my data, and what I do, in conformance with agreed policy
    (Note: There may be non-negotiable elements – I cannot by law forfeit or deny certain rights and duties, say)
  - Measures to control profile aggregation, to avoid and also to clean-up the detritus in the wake of our activities, plus regulatory controls to outlaw intrusive practices.
- Data-protection: clear responsibilities for data-controllers
  - Responsibilities and liabilities;
  - How and where data is stored and handled, and what is permissible (authorised?) use of user-data – what actions and by whom (includes delegation), together with effective controls

2.1 Support for Personal Information Control and Access

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. Tools are required to enable consent management to comply fully with EU D-P rules – eg user access to personal data and to help data-controllers to comply

As in may other topics here, a balance between privacy and justifiable accountability has to be struck.

2.2 Identities and Identity Management

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

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

- Identity provision and global mutual recognition between administrations: official identities, organisation-related identities and roles, personal (cf nick-names) and ad-hoc/temporary/one-time IDs or aliases;
- Management and use of complex/fragmentary/partial identities, including roles, 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 [6] provide guiding principles to how identity is to be protected and respected.

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

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.

"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.

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.

2.3 Privacy and Data Protection

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

2.4 User support and orientation

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

The general usability of the security facilities is critical to success; again this has to provide for the complete spectrum of user-expertise: from the above help for the complete novice to interfaces and toolkits for network administrators.

UI design according to privacy requirements

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

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

Interoperability and consistency of privacy policies calls for tools and standards as in (0), above.

2.5 Trust Management & Governance

Firstly, some 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 could 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, to increase confidence via independent routes.

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, breakdown, and recovery of this trust must therefore be fully supported, with contextualised, distributable, interoperable, and understandable policies in place to implement and manage dynamic trust relationships.

Formal semantics and syntax for trust management and operation are required, capable of differentiation between

- objective assurability against recognised criteria and standards
- subjective trust based on reputation, recommendation, experience, … .

2.6 User-Service Relationships

The user needs service access that provides a proper mutual balance of transparency and accountability with respect to rights and duties. At present, this balance appears to be in favour of the service provider – little more than, for example, **<I accept> – click!** – take it or leave it. 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.

Service providers should be able to present their security policy in terms of claims of the responsibilities and protection that they offer – with respect to, say, the SP's policy for ensuring privacy of personal information, or what protection is offered for corporate data, or the accountability relationship between parties . These claims should be verifiable by the user. The resulting agreements should then be manageable in line with the proposals in 0 above concerning automated policy governance.

2.7 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.

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

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

2.9 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, open, 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.

References

[1] US Cyberspace Policy Review (at 'Executive Summary')

[2] European Directives: *Data Protection* [Directive 95/46/EC] and *Privacy* [Directive 2002/58/EC],

[3] EU Ministerial Conference on Critical Information Infrastructure Protection Tallinn, 27-28 April 2009

[4] The Butterfly Effect: that massive changes may be the result of (sequences of) small, quite random events or actions in the past: James Glieck, *Chaos: Making a New Science* (1987)
however, the converse is that it is generally possible to discover with 20/20 hindsight the route whereby we arrived here (cf weather, financial crisis, …)

[5] RISEPTIS: Research and Innovation for SEcurity, Privacy and Trustworthiness in the Information Society; see http://www.think-trust.eu/riseptis.html

[6] Kim Cameron's Laws of Identity