Project no. 004547

Project acronym:

SecurIST

Project title: Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D *(Steering Committee for a European Security & Dependability Taskforce)*

Instrument: Coordinating Action

Priority: SIXTH FRAMEWORK PROGRAMME

PRIORITY 2

Information Society Technologies

D3.3 – ICT Security & Dependability Research beyond 2010: Final strategy

Due date of deliverable: 30th January, 2007

Actual submission date: 30th January, 2007

Start date of project: 1st November 2004 Duration: 24 Months

Final 1.0

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)	
Dissemination Level:	**PU**: Public
Authors	Zeta Dooly, Jim Clarke, W. Fitzgerald, W. Donnelly, WIT; Michel Riguidel, ENST; Keith Howker, Vodafone
Contributions	SecurIST Partners, SecurIST Advisory board, STF leaders, STF members and other FP5 and FP6 project members involved in ICT Trust, Security and Dependability.

Executive Summary

This deliverable is the key result of the SecurIST Project Work Package 3 – *ICT Security & Dependability Research strategy beyond 2010* – whose ultimate purpose is to create a clear European level strategy to drive ICT Security and Dependability research beyond 2010. Its focus is on medium (up to 3 years) and long-term objectives (~3-10 years).

The document develops the context of the research strategy, setting its objectives, laying out clear objectives backed by detailed content and identifies instruments capable of implementing this strategy. It elaborates upon the Strategic Research Agenda for ICT Security & Dependability Research beyond 2010 facilitating the transition to FP7.

Considerable time and effort has gone into the formation of the Security Task Force (STF) and Advisory Board (AB) in order to reach these goals, this deliverable concentrates on the outputs of these bodies and uses as a basis for its findings the following valuable sources:

- The briefings and outcome reports from the thematic areas
- The technology and business watch reports
- The considered opinions and recommendations of the SecurIST Advisory Board
- The roadmaps developed under call 8 of FP5 and input from FP6 projects
- The outputs of consultation exercises {one to one contacts, networking sessions, discussion workshops – WP2 and WP5)
- Foresight and vision documents (both European and International).

The elaboration and consensus of the key challenges from the different constituencies in a large number of workshops and key events has been a major contributing factor to the contents of this report. The work has been updated considerably since D3.1 Initial Strategy, with the inclusion of three important events, Integration workshop of new Unit D4 projects to the STF, the Joint SecurIST Mobile and Wireless Workshop on Security and Dependability held in March 2006 and May 2006, respectively, and the EU, US Summit on Cyber Trust, Dependability and Security held in November 2006. It was also updated with the final work of the SecurIST Advisory Board.

The main body of the document comprises the higher level strategic view and outputs of the project. The more detailed analysis from FP5, FP6, STF, the AB, and other relevant initiatives is contained in the Annexes. The collective medium- and longer-term background scenario for this report is of increasing complexity, size, and scope of an interconnected digital world, with, on the one hand, increasing heterogeneity and dynamics, and on the other hand, growing convergences and reliance on critical mono-cultures. At the far end of the picture is a possible vision of quantum communication and computing, nano-engineering, and organic components that may call for totally different perspectives. As size and complexity of this digital world grow, so too does our dependency on it for all aspects of personal and public, social and economic activity. This scenario provides an escalating risk of, possibly avalanching, breakdown due to engineering failure or malicious action.

There is, therefore, an even greater need to concentrate attention and effort on the security and dependability aspects and factors in the design and implementation of components and systems, their inter-relationships, and their deployment and usage.

Many of the findings and recommendations of this deliverable call for continuing effort in already established fields – cryptography, trusted components and systems – that provide underlying techniques and technologies. More novel approaches are called for in, for instance, the relationships between the human user and the digital world, with responsibilities and rights moving from central command and control towards the individual, as the boundaries between technical and operational

domains become increasingly fuzzy. Simultaneously, the requirements for increased personal privacy and anonymity must be balanced by the needs of society as a whole for appropriate accountability.

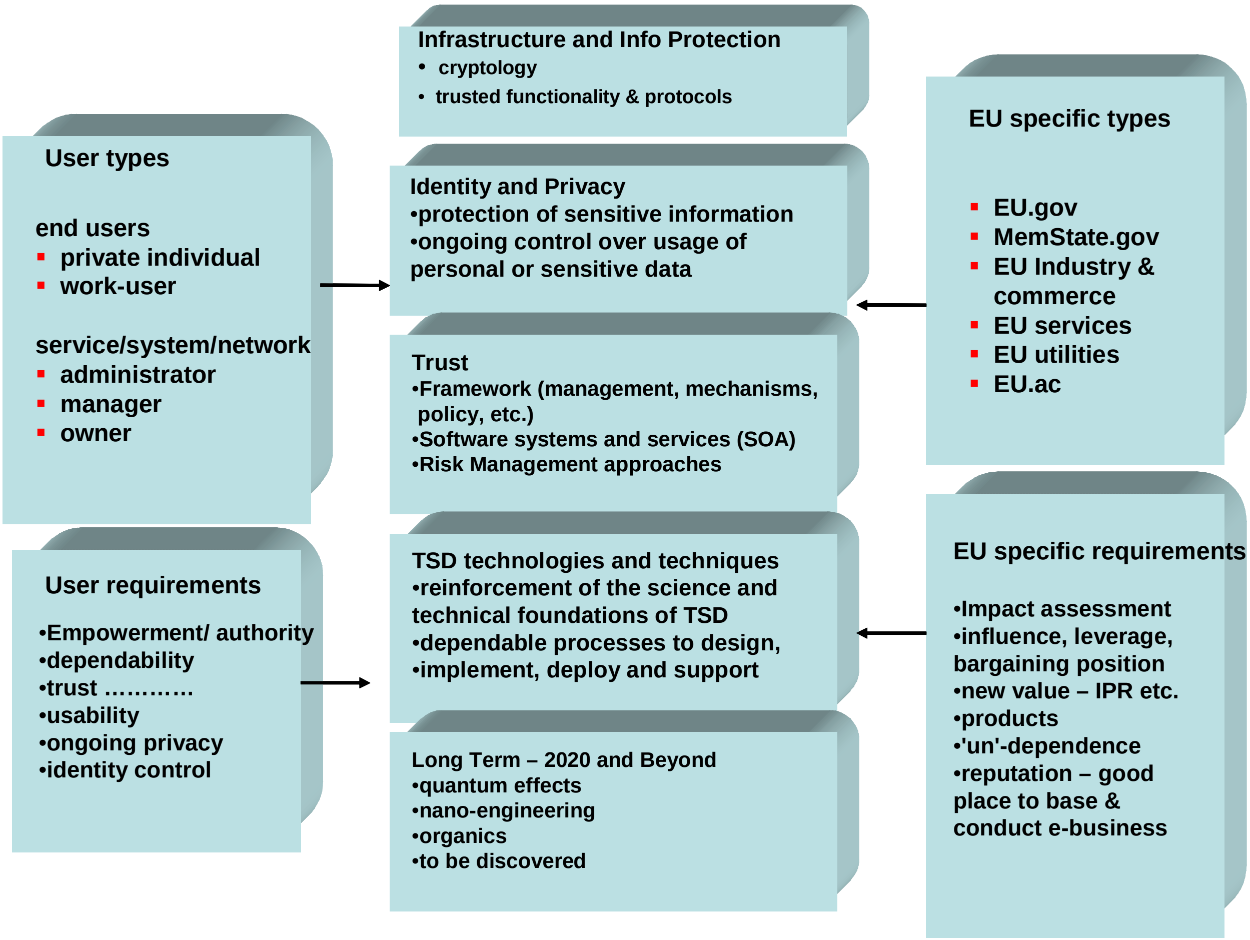

Infrastructure and Info Protection
• cryptology
• trusted functionality & protocols
User types
end users
▪ private individual
▪ work-user
service/system/network
▪ administrator
▪ manager
▪ owner
Identity and Privacy
•protection of sensitive information
•ongoing control over usage of personal or sensitive data
EU specific types
▪ EU.gov
▪ MemState.gov
▪ EU Industry & commerce
▪ EU services
▪ EU utilities
▪ EU.ac
Trust
•Framework (management, mechanisms, policy, etc.)
•Software systems and services (SOA)
•Risk Management approaches
User requirements
•Empowerment/ authority
•dependability
•trust …………
•usability
•ongoing privacy
•identity control
TSD technologies and techniques
•reinforcement of the science and technical foundations of TSD
•dependable processes to design,
•implement, deploy and support
EU specific requirements
•Impact assessment
•influence, leverage, bargaining position
•new value – IPR etc.
•products
•'un'-dependence
•reputation – good place to base & conduct e-business
Long Term – 2020 and Beyond
•quantum effects
•nano-engineering
•organics
•to be discovered

Figure 1 – R&D requirements and drivers

The main actors and drivers and areas for R&D consideration are shown in Figure 1. The *users*, in the left-hand column, irrespective of their role as private individuals or as workers, have the same headline requirements of the digital world: that it is dependable and can be trusted, not least in respecting the individual's privacy and sensitivities.

The motivation for Europe to support this work, shown in the right-hand column, proposes mainly business drivers, albeit with a good tempering of human values, to improve the technological, social, health and wealth of its citizens.

The five central boxes represent the high level view of the main groupings of technical requirements to be addressed by the research programme in ICT Trust, security and dependability as found within the work of the EU Security and dependability Task Force and Advisory Board. In addition, support is needed from the humanities – legal and social issues, and from psychological and physiological insights into a digital future, which is not the main scope of this deliverable.

The research topics proposed by the STF are summarised, associated and mapped with the nine AB recommendations are shown in Table 2 on page 36.

Table of Contents

Table of Contents for Annexes

Table of Contents for tables and figures

1 Introduction

Trust, Security and Dependability (TSD) as a discipline evolves daily, along with the wide deployment of digital (fixed, mobile, wired and wireless) technologies, and their penetration into all aspects of human activity. The advent of ubiquitous computing and communications that facilitate log on and the processing of data in network infrastructures anywhere/anytime, are the main causes of today's growing computer delinquency phenomena. Cyber-crime, the natural extension of real life violence in the virtual world, is compromising the intended handling and operation of digital information and systems.

The evolution of ICT security is governed on the one hand by technological progress (miniaturization of computers, progress in optics) and the consequent emerging vulnerabilities, and on the other hand by the growth in applications, the increased uptake of digital technology in all sectors of the economy and our daily lives and their consequent threats and malfunctions.

The demarcation between physical space and cyberspace will decline by the year 2010. The availability of abundant computing and networking resources, spread of critical data over these resources, and enhanced reliance of organisations and the general public on information technology will attract more attackers as their reward increases. To improve reliability of these edifices, new abstractions must be created in order to invent efficient paradigms; it is also necessary to design new TSD models, production tools using new programming languages, and protocols with modelling, simulation and verification techniques.

The goal of the fast expanding area of resilience research is to strengthen the secure circulation of data on robust networks, the computations of information on secure and dependable computers within a resilient ambience, promote the dissemination of computer applications and encourage the adoption of digital technologies by the large public. In the short term, TSD research must obviously take into account the nature of technological progress and the constantly evolving demand and behaviour, but it must also set itself longer term objectives of a more general nature.

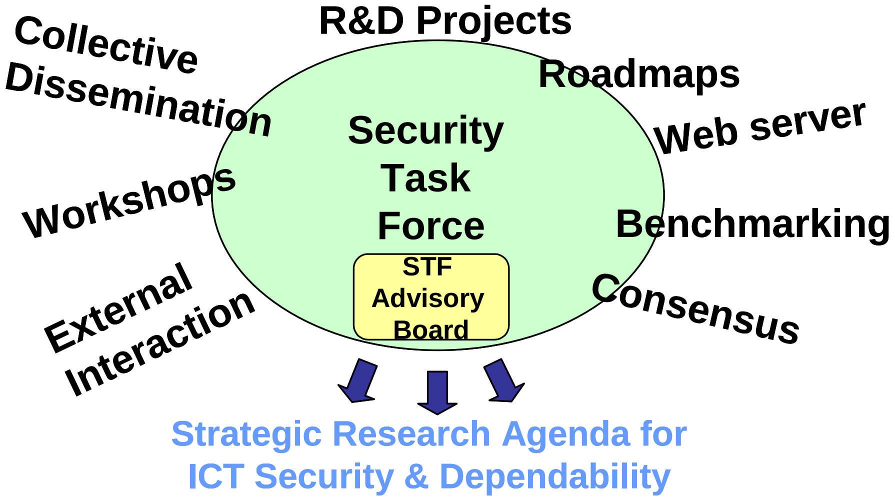


Figure 2 – SecurIST approach

The approach taken by the SecurIST project in developing the Strategic Research Agenda for ICT Trust, Security and Dependability can be seen in Figure 1.

The project established two fundamental bodies – the EU Security and Dependability Task Force comprised of mainly members from former FP5 and FP6 projects and an Advisory

Board, whose interactions can best be described throughout the four project phases in Figure 3.

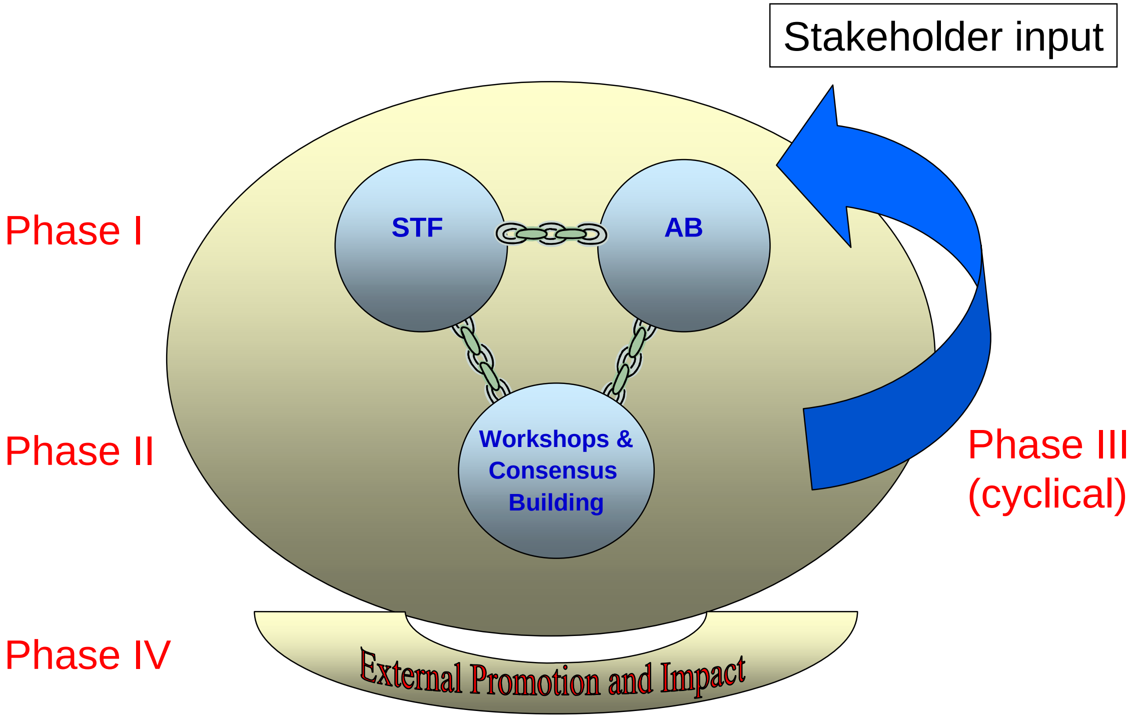


Figure 3 – Interactions between STF and Advisory Board throughout SecurIST.

The following sections contain a description of the roadmapping and consensus building work carried out within the SecurIST project in order to co-ordinate the integration of the TSD communities to highlight the appropriate and necessary strategy for the short, medium and long term areas of research and development that the EU must undertake as it moves into the 7th Framework programme.

After an overview of the roadmapping activities of ICT Trust, Security and Dependability from FP5 to FP7, the recommendations that the TSD community must undertake in future years is set out, and directions for research are proposed. As this deliverable is considered the overall strategy document of the project, the internal contents of the report will contain the higher level strategic view of the project and the detailed analysis from FP5, FP6, STF, Advisory Board and other relevant initiatives are contained within the Annexes of the deliverable. However, this is in no way diminishing the importance of the detailed work carried out by the dedicated members of other projects, Security Task Force, Advisory board and other initiatives. The detailed challenges [Annex II] from the STF Initiatives were presented and reviewed by an esteemed Advisory Board, who published their own Recommendations report (Annex V), which was examined in a consultation forum with the wider community and the final version 3.0 undertook to include many of the useful comments that were made regarding the report. Finally, Chapter 3 provides a summary vision for short – mid and long term research in TSD with a cross-disciplinary view.

2 SecurIST Roadmapping activities

2.1 Introduction

The project undertook to examine the work carried out throughout Framework Programme 5 (FP5) and FP6 starting with the examination of roadmapping activities that were developed in Call 8 of FP5. The project has drawn extensively from these projects, and invited them to bring their experience and drive into the security and dependability taskforce (STF). The SecurIST project followed a transitional approach to achieve its goals as seen in Figure 3.

FP5 Roadmaps → FP6 projects → SecurIST Research Initiatives→SecurIST Advisory Board

The following sections summarise these activities and are divided into 3 distinct areas:

- SecurIST Roadmapping analysis of FP5 and FP6 Projects
- SecurIST Research Initiatives (Challenges identified and prioritised by STF)
- SecurIST Advisory Board (Generation of recommendations report)

2.2 SecurIST Roadmap (FP5, FP6 Projects)

The project first examined in detail the work of the FP5 roadmap projects [Annex I], which were broken down into the following Security and Dependability research areas of coverage as seen in Figure 3, including:

- Cryptology Research
- Identity and Privacy Research
- Dependable & Critical Infrastructure Research
- Mobile, Wireless and Smart Cards Research
- Biometrics Research.

It became quite apparent from the close examination of the FP5 roadmap projects that there were significant research areas identified and there were a large number of FP6 projects generated to cover these areas. It was at this point in time that the SecurIST project became involved with these FP6 projects and there were two initial ground breaking Workshops held in December 2004 - Joint M&W Security Cluster and D4: ICT for Trust and Security [1] and January 2005 [2] in which the Security and Dependability community came together and brainstormed on the formation and make-up of the EU Security and Dependability Task Force.

2.3 SecurIST Research Initiatives

During the formative period of the Task Force, it became clear that it was necessary to expand the original 5 research areas and form additional S&D research initiatives to focus on key research areas.

Following the January 2005 [2] and April 2006 [3] SecurIST Workshops, the research areas were expanded to include research initiatives that were officially formed, launched and populated with members. The SecurIST portal [4] was integral to the facilitation of adding new members and acting as a knowledge repository for documentation The following table shows the Initiatives that were formed in the STF, broken down by the original Security Research areas.

Table 1 – STF Initiatives

Original Research Areas	**SecurIST Research Initiatives**
Cryptology Research	Cryptology Research Initiative (CRI) Digital Asset Management Initiative (DAMI)
Identity and Privacy Research	Identity and Privacy Initiative (IPI)
Dependable & Critical Infrastructure Research	Dependability and Trust Initiative (DTI) Security Policy Initiative (SPI) Security Research Initiative (SRI) Ipv6 Security Research Initiative (v6SI) Security Architecture & Virtual Paradigms (SVPI) Internet Infrastructure Security Initiative (IISI) Application Security Initiative (ASI) Methods Standards Certification Initiative (MscI) Security Risk Management Initiative
Mobile, Wireless and Smart Cards Research	Wireless Security Initiative (WSI)
Biometrics Research.	Biometrics Security Initiative
Total Research Initiatives	**14**

The SecurIST project endeavored to include as many participants and projects within the STF Initiatives and held a special Workshop in March 2006 [5] to fast track the inclusion of the FP6 Call 5 Security and Dependability projects within the Security and Dependability Task force membership. This was a crucial milestone as it enabled the incorporation of a number of other very important challenges not originally captured in the STF work to be included in the analysis by the SecurIST Advisory Board. For example, in the software and services areas, Service Oriented Architecture (SOA) was included in the subsequent output reports. In addition, SecurIST held a dedicated Workshop in May 2006 [6] bringing together the Mobile and Wireless and Security and Dependability Communities for the first time to intensively discuss and agree the mutually important challenges and issues for their constituencies.

The priority challenges identified by the STF as a result of collaboration activities are detailed in Annex III. In Annex IV the challenges are mapped to the AB recommendations in the medium and longer terms

2.4 SecurIST Advisory Board

The SecurIST Advisory Board membership [Annex III] is composed of European experts in Information Trust, Security and Dependability. The Advisory Board carried out the task of reviewing results from the EU Security and Dependability Task Force (STF), and other output from the SecurIST events and activities. The Advisory Board met physically a considerable number of times, at great expense of their time and efforts. They were assisted by the SecurIST project for administration and were provided with necessary travel expenditures.

A large number of detailed challenges and priorities for FP7 were elicited from the EU Security and Dependability Task Force Initiatives and these were presented to the Advisory Board for review both in writing and in presentations at Workshops. The challenges were aggregated and weighted into R&D focus areas by the Advisory Board with the assistance from the STF and discussed at a number of dedicated workshops. The Advisory Board then mapped these challenges to a higher level set of recommendations [Annex IV] and clearly defined these recommendations in a very detailed recommendations report [Annex V] for a future security and dependability research framework in Europe, for the period 2007-2013.

The SecurIST Advisory Board has undertaken the task of examining the requirements for the European Security and Dependability Research Framework from the perspectives of the Information Society's various stakeholders, with a particular focus on those of the individual or citizen within this Society. The information systems that make up the European Information Society in this context consists of hardware, software, processes and people, thus covering non-technical as well as technical aspects. Stakeholders of the Information Society include (but are not limited to) individual citizens, SMEs, large corporations, non-governmental organisations and governments, and indeed the research community itself.

The Advisory Board believe that it is important to address all the different facets of trust, security and dependability in the European Information Society. Dependability is an integrating concept that encompasses the qualities or attributes such as availability, reliability, safety, integrity, and maintainability, and mainly seeks to achieve these attributes in the face of possible accidental physical and design faults. Security is seen as encompassing confidentiality and privacy aspects, integrity and availability of information and seeks to preserve these properties in the face of any threat that may compromise them such as software failure, human error or deliberate attack. The two concepts, overlap extensively, and are closely inter-related. In order to get the maximum benefits of research results going forward, an interdisciplinary and integrated approach is required which goes beyond focussing on narrow technological issues.

There are many stakeholders in the European Information Society and it is important to look at problems, needs and solutions from the perspective of them all. However, the problems and needs of individuals deserve a particular focus. End-users, in particular individual citizens are, understandably, becoming more and more concerned about the increasing complexity of information systems, about the trend toward central control and monitoring in electronic environments and about the continued attempts to make every digitized action accountable by associating it with identities that lead back to individual citizens, corporate entities or members of organisations. To keep up to date with the increasing rate of change of the information society, the end-users find themselves having to put ever more trust into environments they have no way of understanding or assessing. In other words, the risk of using the Information Society's processes and systems appears to be increasing: risks such as identity theft and abuse; disclosure of sensitive information; wrong attribution of charges – *financial* or *criminal*. Currently, such issues are evolving trends only, so for a secure and dependable Europe there are challenges but there are also opportunities. Focused correctly, research for a secure and dependable Information Society can lead the way towards a future environment in which the risks to the various end-users, in particular to individual citizens, of living in the Information Society are significantly lower than they are today.

The Advisory Board has come to the conclusion that given these trends, if there is to be a secure and dependable future Information Society in Europe, the following nine key areas need to be addressed in a European Security and Dependability Research Framework. In addition to these nine key areas, four future *grand challenges* are given that illustrate possible longer-term possibilities and implications. While offering new freedoms and opportunities, they also present new and dangerous security and dependability risks to the individual and to society, and set new challenges to the research community.

Under the headline *From "Security and Dependability by Central Command and Control" to "Security and Dependability by Empowerment"*, the Advisory Board is recommending the following nine key research areas:

1. **Empowerment of the Stakeholders:** Stakeholders of the information society include individual citizens, industry and academia, non-governmental organisations and governments. Empowerment of the stakeholder is vital as there is a clear technological trend towards decentralization of technology, as well as of its management and control. Responsibility, authority and control have to move more towards the end user.

2. ***Europe-specific*** **Security & Dependability:** Europe has a very specific heterogeneous culture and history and set of attitudes to trust and society that requires specific research profiling. Thus, the European Information Society will have the possibility to compete successfully with information societies being established in other regions of the globe if and only if Europe-specific needs are taken into account and actively addressed by technological and socio-technical research projects in a structured manner.

3. **Infrastructure robustness and availability:** As stakeholders come increasingly to rely on ICT infrastructure, covering both local infrastructure such as software, and hardware devices, and network infrastructure, involving various communications technologies, further research efforts are needed for the assurance of ICT network and service infrastructures. Over and beyond ICT infrastructure, there is an evident requirement for reliable and available critical infrastructures such as medical, energy, telecommunications, transport, finance, administration and emergency services.

4. **Interoperability:** The future is unlikely to be a homogeneous, standardized technology for communications purposes, but rather a whole range of fixed and mobile communications technologies, ranging from body area networks to broadband broadcast communications across national borders. If this complex web of technologies is to function effectively, it is crucial that future research focuses on the interoperability between security and dependability technologies and standards.

5. **Processes for developing Secure and Dependable systems:** Research on the systematic improvement of secure and dependable system development (including hardware and software) from their design phase, whether one is constructing an entirely new system, or one composed of pre-existing systems.

6. **Security and Dependability Preservation:** Once systems have been developed and installed, the maintenance of effective system security and dependability is critical. This is particularly true in an increasingly complex world of evolving requirements, technologies and systems. Preserving security and dependability also means preserving the confidence users have with regard to information privacy, transaction correctness, etc.

7. **User-centric security and dependability standardisation:** Strengthen the structured involvement of end users and their respective representatives into relevant standardization activities involving security and dependability technologies.

8. **Security and dependability of Service Oriented Architectures (SOA):** The need to establish and maintain trust and manage policy regulations and service level agreements in an SOA context, together with commensurate advances in software engineering to deliver service expectations.

9. **Technologies for security:** Underlying all of these other research areas is the need to provide higher assurance of trusted communication and handling of digital information. The two fundamental sciences and technologies are (a) cryptology and (b) trusted functionality and computing. Cryptology ensures the protection of information stored or in transit outside a trusted area. The trusted functionality creates and maintains that trusted area, and ensures that information is handled within it as intended, and that the cryptographic processes are correctly executed. Security protocols establish and maintain trusted communication between trusted areas. Both disciplines need sustained R&D to keep ahead of the needs of their dependants.

In addition to these nine key research areas, four future *grand challenges* (covering a 10-20 year vision) are presented by the Advisory Board. They illustrate possible longer-term possibilities and implications.

I **Countering vulnerabilities and threats within digital urbanization**: This challenge addresses open problems that we will face in security and dependability from the expansion and globalization of digital convergence by 2010-2015.

II **Duality between digital privacy and collective security: digital dignity and sovereignty:** This challenge deals with future privacy issues of all the stakeholders, whether citizens, groups, enterprises or states. It addresses the problem of how to override the "Big Brother" syndrome and "dark security", i.e., the future assurance of digital sovereignty and dignity for the various stakeholders.

III **Objective and automated processes – *the Reinforcement of the Science and Technical Foundations of TSD*:** This challenge addresses the problem of how to attain a controllable and manageable world of complex digital artefacts by 2015 and how to inject regular, quantitative techniques and engineering to make the field truly scientific.

IV **Beyond the Horizon: a new convergence – *Going beyond the Digital Universe*:** This last challenge deals with the preparation of a new convergence at a horizon of 2020 and beyond, which is the bio-nano-info-quantum "galaxy" and the new security and dependability challenges that will emerge.

These Grand challenges are explored at greater length in Section 3.8, below.

The Advisory Board also has established and will continue establishing links to other relevant European activities and bodies that are of relevance to security in the future European Information Society, such as the European Security Research Advisory Board ESRAB, and the European Network and Information Security Agency ENISA.

The report of the Board is contained in full in Annex VI – SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework.

In conclusion, Figure 4 contains a comprehensive diagram showing the complete SecurIST roadmap for ICT Trust. Security and Dependability beginning from the FP5 roadmap projects, which resulted in a significant number of FP6 projects, which then led to the SecurIST Research Initiatives that were formed within the STF. The STF Research Initiatives presented their key research priorities and challenges, which were then aggregated, mapped and transposed by the SecurIST Advisory board into nine core recommendations on areas for future research activities and four future Grand challenges for long term research.

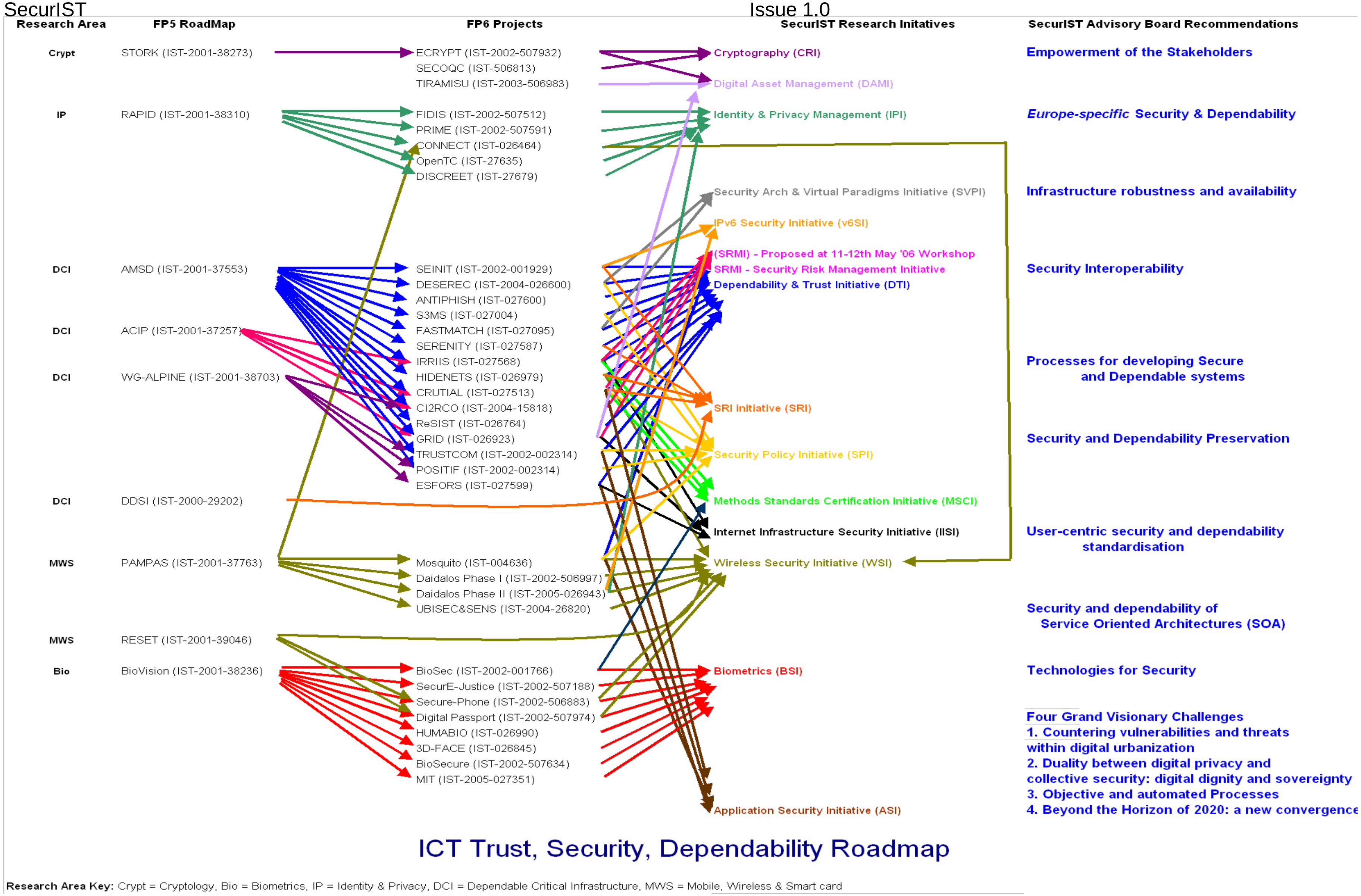

Research Area
FP5 RoadMap
FP6 Projects
SecurIST Research Initatives
SecurIST Advisory Board Recommendations
Crypt
STORK (IST-2001-38273)
ECRYPT (IST-2002-507932)
SECOQC (IST-506813)
TIRAMISU (IST-2003-506983)
Cryptography (CRI)
Digital Asset Management (DAMI)
Empowerment of the Stakeholders
IP
RAPID (IST-2001-38310)
FIDIS (IST-2002-507512)
PRIME (IST-2002-507591)
CONNECT (IST-026464)
OpenTC (IST-27635)
DISCREET (IST-27679)
Identity & Privacy Management (IPI)
Europe-specific Security & Dependability
Security Arch & Virtual Paradigms Initiative (SVPI)
Infrastructure robustness and availability
IPv6 Security Initiative (v6SI)
(SRMI) - Proposed at 11-12th May '06 Workshop
SRMI - Security Risk Management Initiative
Dependability & Trust Initiative (DTI)
DCI
AMSD (IST-2001-37553)
SEINIT (IST-2002-001929)
DESEREC (IST-2004-026600)
ANTIPHISH (IST-027600)
S3MS (IST-027004)
FASTMATCH (IST-027095)
SERENITY (IST-027587)
IRRIIS (IST-027568)
HIDENETS (IST-026979)
CRUTIAL (IST-027513)
CI2RCO (IST-2004-15818)
ReSIST (IST-026764)
GRID (IST-026923)
TRUSTCOM (IST-2002-002314)
POSITIF (IST-2002-002314)
ESFORS (IST-027599)
Security Interoperability
DCI
ACIP (IST-2001-37257)
DCI
WG-ALPINE (IST-2001-38703)
Processes for developing Secure
and Dependable systems
SRI initiative (SRI)
Security and Dependability Preservation
Security Policy Initiative (SPI)
DCI
DDSI (IST-2000-29202)
Methods Standards Certification Initiative (MSCI)
Internet Infrastructure Security Initiative (IISI)
User-centric security and dependability
standardisation
MWS
PAMPAS (IST-2001-37763)
Mosquito (IST-004636)
Daidalos Phase I (IST-2002-506997)
Daidalos Phase II (IST-2005-026943)
UBISEC&SENS (IST-2004-26820)
Wireless Security Initiative (WSI)
Security and dependability of
Service Oriented Architectures (SOA)
MWS
RESET (IST-2001-39046)
Bio
BioVision (IST-2001-38236)
BioSec (IST-2002-001766)
SecurE-Justice (IST-2002-507188)
Secure-Phone (IST-2002-506883)
Digital Passport (IST-2002-507974)
HUMABIO (IST-026990)
3D-FACE (IST-026845)
BioSecure (IST-2002-507634)
MIT (IST-2005-027351)
Biometrics (BSI)
Technologies for Security
Four Grand Visionary Challenges
1. Countering vulnerabilities and threats
within digital urbanization
2. Duality between digital privacy and
collective security: digital dignity and sovereignty
3. Objective and automated Processes
4. Beyond the Horizon of 2020: a new convergence
Application Security Initiative (ASI)
ICT Trust, Security, Dependability Roadmap
Research Area Key: Crypt = Cryptology, Bio = Biometrics, IP = Identity & Privacy, DCI = Dependable Critical Infrastructure, MWS = Mobile, Wireless & Smart card

Figure 4 – Roadmapping activities undertaken by the SecurIST project.

3 Vision of ICT Trust, Security and Dependability for Europe

3.1 Introduction.

In addition to the need for short to mid-term R&D in the nine key areas identified by the SecurIST Advisory Board recommendations report, it was decided that it was essential that a forward watch be maintained that looks out for the possible developments arising from new or emerging technologies as well as new applications of existing technologies. In other terms, we have to build on top of these nine key areas and provide much longer-term reflections and foresight on how the research community may address crucial issues related to the evolution of the Information Society in the coming 10 to 20 years. The four future *grand challenges* mentioned in the Recommendations report are further described below as examples of where possible revolutionary developments might be anticipated.

The purpose of this chapter is to provide a recap of the state of the art and short and mid term vision for Trust, Security and Dependability from the SecurIST project and then examine a potential longer-term cross-disciplinary vision for research in Trust, security and dependability for 10-20 years ahead.

3.2 TSD state of the art in the digital world

Society has become increasingly dependent on digital technology and, thus, increasingly fragile. Major risk is inherent because our daily environment is determined by these complex systems, which can break down or be paralysed by an attack or failure. Since these systems are interconnected and interdependent, they are exposed to a domino effect that could quickly spread malfunctions into the operation of each system. Our attachment and use of 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.

However, threats have now become generalized and hacker software can easily be downloaded from specialized sites by potential delinquents. There are various motives for such attacks: a search for confidential information, the deletion of stored files, the disruption of a network or a server, or the alteration of a web site in order to tarnish an institution’s image. There is, of course, always the lure of financial gain: card fraud, pornographic sites, the sending of spam with the objective of taking in one or two foolish surfers, while at the same time inconveniencing thousands of others. Another form of attack aims at destabilizing users. Viruses, worms and Trojan horses are permanently present on networks, penetrating computers, damaging hard drives’ content and having potentially disastrous effects for businesses.

We live in an increasingly violent world in which the safety of both people and belongings is a growing preoccupation. This violence inevitably exists in the intangible world of the Internet, of mobile telephony, and in the networks and information systems of businesses and institutions, carried out by cyber-criminals, playful hackers, spies, or simply teenagers downloading illegal music files.

To combat this vulnerability, there is a wide range of security tools to protect a file, data, software, a computer, a network or an information system. Security architecture and cryptographic protocols enable trusted links to be established in this virtual world, despite its vulnerability to errors, malfunctions and attacks.

Faced with these threats, large scale information and awareness campaigns, security policies, user charters, and risk management strategies have been developed and have already had a profound effect on user behaviour, predominately within industry or public institutions. However, the construction of a dependable and secure computing world remains a challenge.. Trust in these complex systems is a key factor in the success of these new technologies.

Computer security has profoundly changed in scope during the last ten years. Security is now a multidisciplinary activity: classical cryptography, formal mathematical methods, electronic watermarking, biometrics, network engineering, various security mechanisms (smart-cards, firewalls, intruder detection systems, honey pots, biometric devices), security infrastructure (certificate management for identification and authentication of entities in commercial electronic transactions), trust infrastructure for electronic exchanges (electronic signature of contractual documents), surveillance systems, legal aspects, methodologies for validation of assurances of security, crisis management.

Security has itself become a source of mistrust. Publishers of security software must be trustworthy and not include functionality that will enable them to spy on their customers' behaviour. For example, some unscrupulous companies selling Spyware software place Spyware code on potential consumers machines purposely (e.g. code that opens their CD ROM drive) and use this to point out to them that their Spyware removal software, if purchased, will remove this code. Security on a just-in-time basis, such as the constant updating of antivirus software for computers, is also vulnerable.

With the increased level of computerization, digital traces are left by users, without their knowledge, of every transaction carried out within an information system. As a result of the growth of embedded computing and mobile technologies permanently connected to a network, it has become possible to identify and locate an individual in various ways.

Electronic traceability is increasingly a threat to our freedom as citizens and to our private lives, and to legitimate and vital business and governmental activity.

3.3 Assurance versus security and dependability

The implementation of security functions such as identification, authentication, access control, and data protection can be viewed in terms of a security assurance model. This model relies on the security architecture of a system, which in turn is based on a trusted infrastructure. This assurance model is, therefore, at the heart of security and privacy, in fact defines its existence, the level and features of the protection it offers, and determines the need and relevance of the deployment of specific security mechanisms. In turn it supports the protection and integrity of the digital world, and hence its dependability.

It is possible to separate the trust providing assurance model and the security architecture, into two separated distributed entities (instrumentations, protocols, architectures, management). This would allow us to automate and boost the trusted infrastructure and security infrastructure, while the authorizations, exceptions, and security management as a whole, are achieved through their interaction. Figure 5 illustrates these trust and security entities and their environmental links.

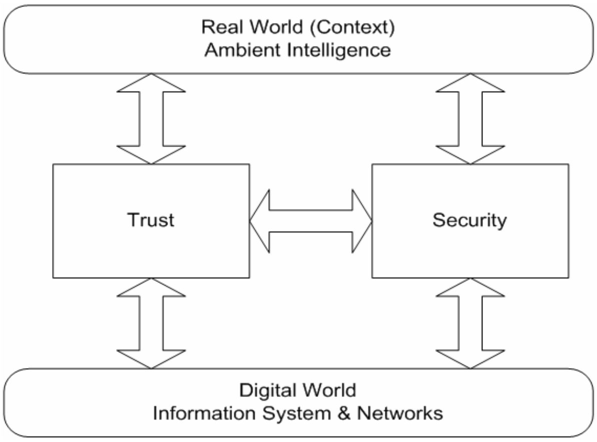


Figure 5 – Dissociation between both Infrastructures & Instrumentations of Trust & Security/Dependability

3.4 Vulnerability and fragility of digital infrastructures

3.4.1 Introduction

In the last decades, we have seen the collapse of borders allowing free circulation of goods, people, and ideas. Digital systems are no exception to this rule. An evolution of services, infrastructures, networks and computer architectures is taking place around more nomadic users, characterised by wireless communications, and mobile or movable components, modular computer hardware, mobile software and fluid data. Large digital infrastructures are being deployed as a result of the success of the Internet. A heterogeneous interconnecting and interdependent digital web is being spun, meshing global accessibility, and providing ubiquitous access and communication. At the same time, large meta-computing initiatives are being launched to harness the power of this ubiquitous computing infrastructure.

ICT security must balance personal freedom and the need to protect tangible and intangible assets and resources, supporting this through measures to correct software programs, by increased robustness of architectures and by ensuring the immunity of applications and the resilience of systems. This balance instils and preserves trust and confidence in digital critical infrastructures and in the applications and services they offer.

3.4.2 Threats and vulnerable evolutions

Today, modern attacks have a broad range of motivations: to gain knowledge from data, alter or destroy a file, tarnish a company's image, tarnish a person's reputation, destabilize an institution or a country. One can expect attacks to further intensify in the future as attackers gain experience and the supporting IT improves. Globalization has changed the stakes, generating new forms of aggression. After the recent dramatic events in New-York, Madrid and London, the world has entered into a new era where conflicts will be less rooted in territorial stakes and increasingly involve the rejection of traditional value systems. "Symbolic" wars, using digital technologies, led by small highly-motivated groups with few resources, may take on a brand new dimension once digital convergence is fully established, and distributed ICT is fully operational.

As a result of the growth of embedded computing and mobile technologies permanently connected to a network, it has become possible to locate an individual in various ways. Telecoms operators have data on the location of a customer's phone, internet service providers can record which sites their customers visit, and banks know when and where transactions are made electronically. In short, detailed electronic trails are constantly generated in real time, without our knowledge, and these may be put to good or ill use.

Despite the unquestionable success of digital technology the resulting information systems are vulnerable and fragile because it is in the nature of their construction that the digital content is independent of its physical support. The digital world is, thus, volatile: content (data, software) can easily be duplicated or destroyed; it can also be falsified. Furthermore, since digital documents are read and written with equipment that uses software and that are designed using software, and software nearly always contains errors or bugs, the possibility of some kind of malfunction is ever present. In some cases invisible vulnerabilities may have been designed into systems

3.4.3 Threats

Potential threats against the correct operation of networks, systems, and infrastructures are varied and range from ordinary failures to technical malevolence and to human clumsiness.

The construction of cyberspace involves a process of trial-and-error and when it has negative consequences, these must be faced and resolved. The threats materialize through the emergence of sites hosted by suspect servers; the use and partial obstruction of networks in the form of illicit contents and unsolicited messages (spam); the pollution of mail servers; the propagation of viruses; the illegal downloading of audio and video files; the circulation of false information; the intrusion of hidden information and malicious software programs (spyware and malware); fraudulent activities such as identity theft and phishing; and, the creation of havens for cults, mafias, and a refuge for cyber-crime and cyber-terrorism. The impact of these incidents and aggressions can be severe in economic, social and legal terms.

Audiovisual and multimedia industries face most of the aforementioned security issues. In the specific context of their trade, the intangible nature of content necessitates not only acceptable responses to hacking phenomena, but also to guaranteeing their traceability and seamless integration into the production processes, as well as their transparency for legitimate end users.

3.4.4 Violation of individual freedom: electronic shadowing

In the digital world, there are actual threats against the private sphere, be it that of natural persons or legal entities. Such threats are created by the digital traces we leave when we navigate in the virtual world. Electronic shadowing is an unavoidable threat and sources of traceability of our everyday activity are amplifying: GPS tracking, localization through mobile telephones recorded at telecommunication companies, and credit card payments in various shops, or the myriad of photographs memorized by city cameras. Nowadays, every citizen is recorded into approximately 500 files, any individual circulating in a major city is filmed dozens of times per day, by public or private entities, and communications of every mobile telephone user are recorded. While all these are motivated by the effective localization of criminals or terrorists, they may also be easily misused to find out about our private activities, if insufficient attention is being paid to protecting our fundamental rights, private activities and personal data. To avoid such risk, it is necessary to establish a strict regulation of the utilization of specific files and of the traceability records of individuals and goods they carry.

3.4.5 Defective system design and manufacturing

The digital world we have built so far is fragile and vulnerable. The main causes for this are an incomplete knowledge and control of underlying infrastructures by ICT system and network designers, manufacturers, and vendors, and the lack of transparency for users. The reasons are technological[1], practical[2], economic[3], and sociological[4]. Moreover, the engineer who designs a system or service has become an architect that has lost control of his building blocks and consequently, the security of the infrastructures is often built on quicksand. The integration of components is performed more according to deadline obligations and cost objectives rather than addressing thoroughly all the security challenges. The main concerns are directed to interoperability and compatibility rather than security and operational reliability[5].

Overall, the accelerated pace of technological development does certainly not promote the deployment of mature solutions. The international community’s digital governance will sooner or later have to take seriously into consideration the matter of digital economics and security on a global scale.

[1] The semantics of procedural programming languages.

[2] Due to the lack of proper and effective software development environments, the defects in the prevailing software systems design and development methodologies, etc.

[3] The economic models of software packages sold and marketed today are very often revised versions following user feedback.

[4] Appropriation of digital technologies by a small part of the population.

[5] The operating dependability of large systems, like the Internet and the GSM networks deployed in the 1990s, has declined when compared to that of older infrastructures, such as fixed telephone or power distribution systems.

3.5 Short – Mid-term research and technology Roadmap

The evolution of our digital society is characterized by ubiquitous computations, communications and storage, and by the development of services that are personalized and context-aware. The trend is towards the emergence and deployment of ever more massively distributed, interoperable and interdependent complex ICT systems composed of billions of interacting components both fixed and mobile. Their emergence will create new, unprecedented challenges for Trust, Security, and Dependability and Privacy.

In the near future, the effects of ambient intelligence and ambient networks will be felt, with embedded sensors and devices forming ad-hoc networks requiring new mechanisms for establishing trust when sharing information or resources. New paradigms come to the foreground, such as service architectures that compose services from lower level modules using federation and mashing-up. Peer-to-peer systems characterized by their remarkable robustness and resilience against attack will appear, with biological-like defence mechanisms, which may go on to inspire new breakthrough technologies. At a larger scale, the completion of the Galileo satellite navigation system around 2009 will create ever more sophisticated possibilities for positioning with implications for both security and privacy.

The goal of the fast expanding area of resilience research is to strengthen the secure circulation of data on robust networks, the storage of data and the computations of information on secure and dependable infrastructures within a resilient ambience, promote the dissemination of services and computer applications, and encourage the adoption of digital technologies by the general public.

The future evolution of networks (future Internet, new Telecom Infrastructures) and services (Grids, overlay services) will involve technical, behavioural, organisational and even psychological changes, as evidenced by the growing dependence of our everyday activities on ICT systems.

Companies are said to be agile, with short reaction loop decision cycles and just-in-time procurement cycles. Meanwhile, ICT providers evolve toward dynamic reconfiguration of customised services, and security also evolves towards just-in-time (software and antivirus developments). However, its effectiveness will be more and more precarious and there is a need to move towards real time reaction capability to face the growing threat and fragility.

The security of the dynamic reconfigurability and update of hardware, software, applications and services (spontaneous virtual applications created by end users) at runtime is a major challenge for the years to come.

Our vision for the resilient systems of the future consists of cross mechanisms to link the virtual interfaces of:

- overlay services (computing systems such as Grids),
- overlay networks (communication systems), and
- peer-to-peer structures (e.g. mass storage systems)

Common security mechanisms mainly based on boundaries and firewall protection mechanisms do not scale with respect to new complex pervasive systems. We should imagine different mechanisms such as those based on analogies with the bio-living world, (e.g., immune and self-healing systems), as well as autonomic, evolvable and adaptive security mechanisms. This will definitely require new cognitive techniques and semantic models managing the complexity of ambient environments where people/devices may jointly act and interact.

Mechanisms and tools are needed for assessing and proving the security and dependability of a complex system. The scale of new ICT systems and the kind of threats or faults and assumptions on their operational environment pose new challenges and the need for an assessability discipline is even more impelling. Different metrics, modelling tools and observation mechanisms are needed. The capability of measuring the tolerance to attacks or to faults is crucial in new systems that due to their logical and physical diffusion are likely to be under constant attack.

Future ICT systems will involve thousands of millions of devices (RFId tags, smart networked sensors), including nomadic devices, as well as huge virtual entities (such as Virtual Private Networks and Overlay Networks), and will no longer be able to depend on setting boundaries for their security. Instead, they will require a capability for managing and negotiating trust relationships, adapted to the level of security required in a given situation. The understanding on how trust emerges and evolves as well as of related notions as reputation formation, monitoring and evolution are mandatory. The challenge is then to obtain a greater understanding of partial trust, security-based trust (where trust follows from security), and trust-based security (where security is achieved through a trusted partnership), and to use this understanding to realize a high level of trust of the citizen in the deployment, economic viability and social acceptance of systems and services. This will require expertise and joint research in several fields beyond ICT, such as economy and sociology.

In order to construct resilient architectures of large evolutionary systems (International Enterprise Information Systems, Computing Grids, Web Services, etc) made up of independent heterogeneous elements that are context aware, have adaptive behaviour and take into account mobility, dependability and security, we need to develop new computing, communication and information models, taking into account security, dependability, trust and privacy. These models must be sometimes discrete, sometimes continuous and sometimes stochastic to envisage the future and explore the environment. With all these disruptive models, it will be possible to design and build new architectures, new protocols, and new trusted infrastructures. New languages and tools will also be needed. This involves the creation of programming and mark-up languages and tools; and interaction languages and tools.

Therefore, before 2010, research will mainly focus on developing established lines of research[6]:

- Ambient Intelligence security and virtual security: new security paradigms that meet the requirements of ubiquitous applications, service oriented architectures, establishment of trust without basing oneself on an existing infrastructure or organisation, low connectivity or intermittent connectivity structures, medium guarantee level as compared to the ordinary search for absolute assurance;
- Resilience, security and dependability of large critical infrastructures: The management of crises amplified by the domino effect; the protection of critical infrastructures and methods and tools for making them resilient;
- Modelling and implementation of security policies: introduce the space and time, the context and the mobility, manage security policy conflicts, and model large infrastructures and security policies for health and medicine and for public administrations;
- Cryptology: cryptographic mechanisms that require less resources, particularly in a constrained environment; cryptographic mechanisms for rights and assets management (DRM and DAM) guaranteeing their traceability; and flow encryption methods that are as safe, yet more effective, than current block encryption methods;
- Biometrics: large databases for the calibration and benchmarking of recognition algorithms, signature with biometrics, behaviour recognition by following a person and analyzing its gestures;
- Identification and authentication of players, contents, and rights management;
- Network security: fixed and wireless, mobile, active, ad hoc;

[6] Detailed challenges from the EU Security and Dependability Task Force can be found in Annex III.

- IS security: techniques for intrusion detection, privacy protection, grid security, bait system architectures;
- The realistic assessment of vulnerabilities from the operational point of view, virus stopping, spam screening upstream from the end user's terminal;
- Certification, the assurance of security: introduction of incremental, faster and less costly, security assessment methodologies.
- Watermarking of images, sounds, video data flows, and software programs: protection of assigns, control of copies, authentication, integrity;
- Steganalysis: detection of hidden data using steganographic methods;

While considering the short to mid-term evolution of both technological and socio-economic aspects as presented above, the goal is to build on top of these and provide much longer term reflections and views on how the research community may address crucial issues related to the evolution of the Information Society in the coming 10 to 20 years ahead. In this context, the next sections discuss the main research directions of work that have been identified for the (r)evolutionary period.

3.6 Overview of Long term vision of security challenges.

The disciplines required for digital security and dependability must continuously evolve and keep abreast with (or better, ahead of) the widening deployment of digital – fixed, mobile, wired and wireless – technologies, and their penetration into all aspects of human activity.

The goal of the fast expanding area of Trust, Security and Dependability research is to strengthen the secure handling of data on robust networks, the computations of information on secure and dependable computers within a resilient ambience, promote the dissemination of computer applications and encourage the adoption of digital technologies by the general public, and provide effective means of trust and risk management.

Computing is not a discipline that is governed by the laws of nature[7]. It is a pure creation of the mind, with all its advantages (inventiveness, originality) and faults (errors of strategy, price-fixing, forecasting, specification, design, validation, operational use, etc.).

To grasp the complexity and follow the construction of these digital structures, new abstractions must be created in order to devise new efficient paradigms. It is also necessary to design new models, production tools with new languages, and protocols with modelling, simulation and verification techniques.

In order to construct resilient architectures of large evolutionary systems made up of independent heterogeneous elements that are context-aware, have adaptive behaviour and take into account mobility, dependability and security, we need the following:

first, research on **new computing, communication and information models**, taking into account trust, security and dependability.

second, the **injection of semantics** into these systems, because in a mobile, changing world, information must be validated **locally**. These models must be sometimes discrete, sometimes continuous and sometimes stochastic to envisage the future and explore the environment.

third, the creation of **interaction models and knowledge models** so that independent devices can, during their life cycle, learn how best to interact; also **models for creation, acquisition, distribution, sharing of knowledge and trust**.

[7] apart from the fundamental law of engineering: *what can go wrong probably will*

With all these diverse models, it will be possible to design and build new architectures, new protocols, and new trusted infrastructures.
To carry out such work, we need also to spend efforts on **languages and tools**. This involves the creation of programming and mark-up languages and tools, interaction languages and tools, in order to inject security and dependability during the design phase. New trust, security and dependability infrastructures with separated instrumentations and processing are required, in order to better grasp the digital activity, and to better understand the validity and the quality of trust. It is also necessary to develop protocols in much more flexible and decentralized networks that will break the monotony and symmetry of network nodes, with algorithms of cooperation, coordination and autonomy, thus resolving issues of scale.

fourth, and finally, **assessability** (**verification and validation**) **techniques** need to be developed.

In the future, it will not just be individual computers that are targeted by hackers. One has to reckon with a rapid increase, for example, in attacks on name servers (Domain Name System or DNS), which are responsible for allocating host names to IP addresses. Attackers are increasingly focusing on routers, firewalls and other security tools, which are intended to protect the systems of companies and administrative bodies. Such attacks have a new detrimental quality since entire computer networks are affected by them.

The demarcation between physical space and cyberspace will fade away by the year 2010. The availability of abundant computing and networking resources, spread of critical data over these resources, and enhanced reliance of organisations and the general public on information technology will attract more attackers as their actions become more rewarding.

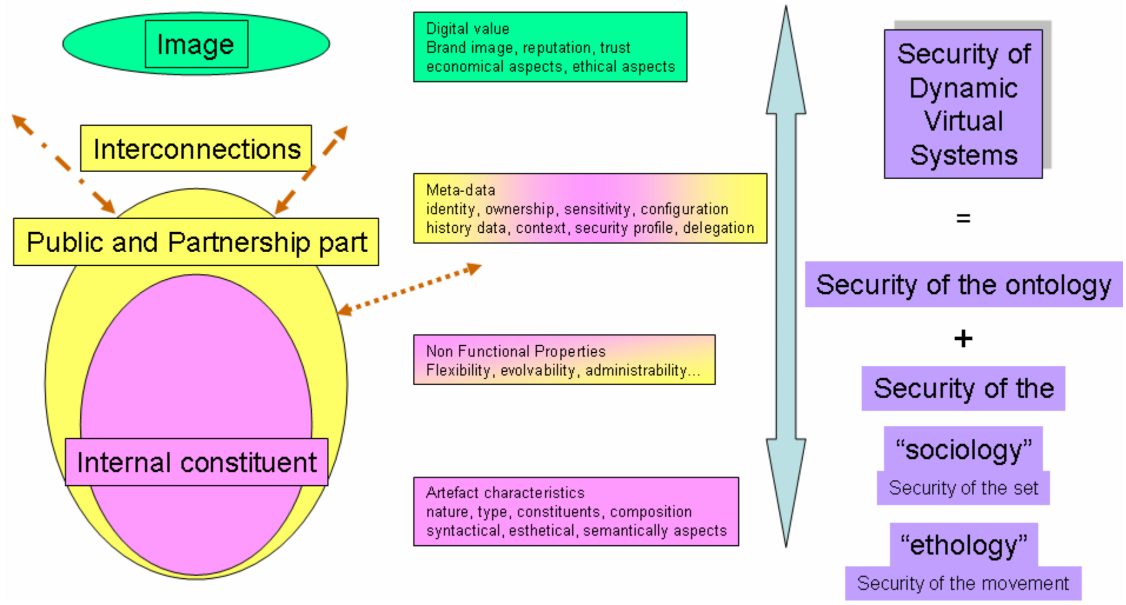


Image
Interconnections
Public and Partnership part
Internal constituent
Digital value
Brand image, reputation, trust
economical aspects, ethical aspects
Meta-data
identity, ownership, sensitivity, configuration
history data, context, security profile, delegation
Non Functional Properties
Flexibility, evolvability, administrability…
Artefact characteristics
nature, type, constituents, composition
syntactical, esthetical, semantically aspects
Security of Dynamic Virtual Systems
=
Security of the ontology
+
Security of the
"sociology"
Security of the set
"ethology"
Security of the movement

Figure 6 – Trustworthiness and Security

3.7 Social and technology trends

3.7.1 Digital convergence

As shown in Figure 6 above, digital convergence is continuing the inevitable process of abolishing the boundaries between the three digital industries (computing, telecommunications and audiovisual), to create and harmonize an end to end value chain with interoperable infrastructures, configurable architectures, flexible services and compatible terminals. This is emerging in the form of a universal network to which one connects in order to obtain services, but is also necessitating a brutal confrontation of standards (e.g. communication standards in the lower layers, operating systems of terminals), a ferocious struggle in markets (e.g. voice over IP and telephony), massive change in behaviour and uses (e.g. high speed internet access, downloading of music files and the delayed explosion in e-commerce) and a profound change in the entities and economic rules involved (e.g. the appearance of recent giants such as Google, or of innovative and highly successful services such as Skype).

3.7.2 Ambient intelligence

New paradigms are emerging that respond to the complex demands of proximity and use. This encourages the IT and telecom industries to develop new solutions that combine technology and markets with geography and users. Among these ideas, the concept of ambient intelligence underpins the provision of dynamic digital services to users anywhere, anytime. At the same time, we witness the emergence of networks of sensors and actuators - "smart dust" that are spreading out in the urban landscape and are operating like smart labels.

Such ambient systems have built-in intelligence. They are networks featuring specific entities that provide intermediation services to assist communications (bandwidth brokers, localization servers, memorization of node topology) or to facilitate terminal operations (configuration, service discovery). An ambient network can also use external services (management of time, space, wireless resources). Intelligence is built on top of the computational and/or communication infrastructure, and applications will be configured according to their geo-localized use. Delivery of information is hence facilitated by cooperation at multiple levels.

3.7.3 Embedded systems

Embedded systems are independent entities, which accomplish a specialized task, sometimes critical, without human intervention, generally in direct interaction with the external physical or computing environment. These miniaturized independent systems may be isolated but are usually connected and communicate through a network. These systems are subject to operational constraints which affect their definition, robustness, design and capacity to accomplish a task with defined resources, often linked to time constraints or energy consumption.

3.7.4 Critical and interdependent infrastructure

The ICT infrastructures described above are becoming the economic nervous systems of nations. The control of a nation's physical infrastructure and services is integrated with into this nervous system and its availability and correct operation. Cyber-terrorism is a fundamental threat to modern societies. The international interconnection of networks and the development of information technology has added multiple, dangerous international dimensions to computer crime.

Critical infrastructures have elevated requirements on security and availability. However, where security and availability are issues, security assurance evaluation becomes crucial. Evaluating security assurance is a non-trivial problem. In this paper, we discuss several security assurance aspects and the role of modelling in this context. We then introduce a novel, non-intrusive approach to security assurance evaluation. This approach comprises an infrastructure modelling technique, the additional evaluation infrastructure, the evaluation methodology and possible implementations in an existing network.

In terms of security, the increased heterogeneity increases the complexity of the main security functions such as identification, authentication, access control, and data protection. The implementation of these functions generally and objectively derives from a security assurance model epitomized by a trusted infrastructure that, in itself, represents the basis of the security architecture. Assured security and dependability is therefore at the heart of safety of the infrastructure, as its existence, its level and/or features; determine the need and relevance of the deployment of such and such other security mechanism, and vice-versa.

3.8 Security, Dependability Trust, and Privacy – four Grand Challenges for Long Term R&D

In this section, four *grand challenges* that TSD science must take up in future years are given as examples of where possible (r)evolution might be anticipated. These challenges are based on a cross-disciplinary perspective and reflect the preparation of appropriate reaction to potential future dark visions and golden opportunities. These grand challenges are not imaginary, but are very real possibilities. Underlying R&D directions on which they are based may look as FET-like research and beyond, but the outcomes will be very tangible. The security and dependability community needs therefore to be vigilant on these; the options for response to resultant opportunities and threats need ongoing investigation.

3.8.1 Grand Challenge 1. Countering vulnerabilities and threats within digital urbanization

The **first grand challenge** is the Trust, Security and Dependability improvement for the expansion and globalization of digital convergence by 2010-2015. It is relevant to observe three inter-related phenomena:

first, the boundaries between physical space and cyberspace will diminish;
second, the dependence of citizens and organisations on ICT will increase so that it is crucial to enhance Critical (Information) Infrastructure Protection; and
third, threats and vulnerabilities will increase while service availability will likely decrease; more specifically, when we consider the figure 99.9…9% of availability for a system or a service, the question is how many 9s are required? how many will be really implemented? and what is the consequence of the 0.00..01?

The above can be translated to the following challenges and issues for the TSD community.

- ***how to move from "claustro-security" (closed and ciphered world) to an "agora-security" (open and clear world)?***
- ***how to move from static and standalone activities to a collaborative, network centric architecture vision with full mobility and full interactivity with people and reality?***
- ***how to make the actors' chain proportionally responsible and accountable for malevolent or erroneous actions?***

The evolution is towards ICT infrastructures that are globally interconnected and emerging as the economic nervous systems of the modern world. The information society is, thus, becoming ever more complex but also more fragile. Cyber-terrorism and computer piracy is set to increase. This will threaten our society and affect the daily lives of our citizens, the management and lives of our enterprises, and the operation of governments.

A vast number of interdependencies are progressively being built between the different information and communication systems and the various areas of human activity, such as administration, banking, energy, transportation, public health, and defence. Two trends seem then to emerge:

- Dependence on vulnerable, interdependent, interconnected, complex ICT systems: the information society evolves towards a more interconnected and standardized world. This evolution is characterized by an increasing use of 'open' communication infrastructures, such as the Internet, but also by a widespread use of monoculture software applications. This brings about vulnerability to all kinds of accidental or deliberate incidents and aggression, and their rapid propagation through heterogeneous infrastructures that operate more and more interdependently and under the same standards.

- Real-time resilience and security: The future evolution will involve technical, behavioural, organisational and even psychological changes, as evidenced by the growing dependence of our everyday activities on ICT systems. Companies are said to be agile, with short reaction loop decision cycles and just-in-time procurement cycles. Meanwhile, security also evolves towards just-in-time (software and antivirus developments). However, its effectiveness will be more and more precarious and there is a need to move towards real time reaction capability to face the growing threats. The security of the dynamic reconfigurability and update of hardware and software at runtime is a major challenge for the years to come.

3.8.2 Grand Challenge 2. Duality between digital privacy and collective security: *digital dignity and sovereignty*

The **second grand challenge** is privacy issues of all the players (citizens, groups, enterprises, states).

There are always two perspectives in terms of security: the point of view of the user who wants to protect himself against the network (this is the digital privacy standpoint, with a requirement for the preservation of individual freedom) and the point of view of the network or society. This needs to protect itself against malevolent and irresponsible users (this is the ambient security standpoint, with a requirement for the protection of the community).

The question for the ICT usage is the assurance of digital sovereignty and dignity for citizens and groups:

how to override the “big Brother” syndrome and the dark security?

One can thus picture the subtle and tough competition between the methods designed to preserve a subject’s privacy and the legal procedures to watch such subject and, the practices intended to preserve the rest of the world against the potential malevolent or accidental acts of such subject, and the latter’s remedies to find out what means are being implemented to control him/her. Creating a climate of mutual respect and trust is not detrimental to the setting up of mutual defence cross-procedures. Transparent dialectics should make it possible to negotiate the rules and subscribe to clear and harmonious security policies. Such digital dignity is the price to pay for the democratic values of our civilization.

The values of modern civilization are inevitably moving towards an immaterial world. Continuous electronic miniaturisation, the acceleration of communication networks’ performances and the inexorable deployment of computing infrastructures is creating a digital urbanisation, 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 organisations) 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 digitalization 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. 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 his knowledge, someone’s personal computerized data.

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

The security of the digital world has become a fundamental stake for the **citizen** with respect to his individual freedom and protection of his 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: electricity and water distribution systems, communication methods and means, and information and communication systems pertaining to these infrastructures.

There are always two angles of view in terms of security: the point of view of the user who wants to protect himself against loss of control over personal data when operating in the network and the point of view of the network or society, that needs to protect itself against users who are irresponsible or have malicious intentions. The latter is the ambient security standpoint, which is based on the need to protect the community.

This illustrates the subtleness 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.

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. 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 global dimension and is used by a broad 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.

3.8.3 Grand Challenge 3. Objective and automated processes - the Reinforcement of the Science and Technical Foundations of TSD

The **third grand challenge** is the obligation to attain a controllable and manageable world of complex digital artefacts by 2015 toward a provable security environment (predictability of faults, anticipation of threats).

The challenge is the measurability issue:

> ***how to establish quantitative techniques and engineering to make the field of security and dependability truly scientific?***

Security is still an engineering craft and not yet a science. The security policies are still descriptions and declarations rather than precise specifications. Security is not yet a Turing machine, attached to a system to protect it. The digital world is a tower of Babel of languages and ontologies with radical different statistics, scales and sizes – and opinions.

Couple this with the explosion of content, the architecture of data and programs associated with an individual or an organisation has become rhizomorphous[8]. This consists of “bulbs” of data and programs, which (due to the convergence of computing and telecoms) are in the process of being generated and stored, sometimes without their owner’s knowledge. There is a genuine concern facing the digital urbanization that is taking place: the perplexity of users, and also the difficulties of developers and operators. Users will soon have a new ecosystem, an immense communication machine which will be able to link human nomads and their interconnected everyday electronic devices. We are witnessing the birth of a digital kingdom made up of independent entities, which live their own life cycles. The prospect of this generalized network communication, with no hierarchies, in this new kingdom, raises theoretical, technical and ethical issues that remain unresolved:

- The disappearance of impermeable partitions separating private, professional and public life. Within this unique common infrastructure, all individuals build, as an extension of their being, private virtual networks of their own data. These networks will begin in digital prostheses in the biological body and finish by dispersing in the far reaches of the planet in the chaotic mass of the undifferentiated digital slurry of fungible information on the web. These networks linked to individuals are permeable, vulnerable and ultimately move beyond their control. Individuals also leave tracks, indelible digital traces that other humans can subsequently use to construct a biography without their knowledge.
- The complex construction on top of the physical world of several floors of virtual logical worlds, each one more symbolic and more abstract. The new computing consists of attaching, at whatever cost, the various floors in these virtual interlacings to real physical events, in order to connect with the real world. The designers of these edifices are prisoners of these paradigms, which accumulate over time as technology evolves and which ultimately paralyze the success of digital techniques;
- The construction of a mass of data (with nuggets of information buried in a chaos of essentially discarded information) which is visibly growing and which non-specialized search engines have difficulty conquering: fungible information, run-of-the –mill information of all kinds that has to be searched, captured, sorted, selected and checked, thereby creating a pervasive entropy;
- The elimination of borders between entities:

[8] Root-like in form.

- geographical entities such as states (the Internet ignores countries' topographies and defies national boundaries), businesses' information systems (computing is increasingly outsourced), inner sanctuaries (radio waves extend beyond the walls of our physical constructions);
- temporal entities such as meetings in the flesh and live discussions; mail and forums have resulted in an explosion in the number of meetings and conversations that take place on a non-temporal basis;
- computing entities which dissolve in an indescribable syncretism with distinct but intermixed ontologies, like the construction of interoperable encapsulated protocol entities, which become entangled and interdependent.

The following areas are identified as specific research challenges for the long term within this overall challenge:

1. Resilience techniques (trust, security, dependability and privacy)

The mass diffusion of digital systems must be endorsed with built-in mechanisms for enhancing confidence in their usage. The following main issues need to be tackled:

Networking aspects**:** Common security mechanisms mainly based on boundaries and firewall protection mechanisms do not scale wrt. new complex systems. We should imagine different mechanisms such as those based on analogies with the bio-living world, (e.g., immune and self-healing systems), as well as autonomic, evolvable and adaptive security mechanisms. This will definitely require new cognitive techniques and semantic models managing the complexity of ambients where people/devices may jointly act and interact.

Security for small devices: Security systems and cryptographic mechanisms must be scaled down in order to be inserted in small devices (even at nano-scale). Tiny devices will definitely have specific requirements such as energy consumption, computation power, and so forth. Efficient, flexible and scalable low-cost cryptographic protocols and mechanisms must be developed and combined in order to create a secure and dependable Ambient Intelligence space as well as ensure privacy protection.

Secure and dependable software: We need also to develop a discipline of system and software security based on the development of methods, tools, and repositories for high-level verifiably secure programming. We advocate an approach based on efficiently verifiable mathematical proofs showing compliance to policies, expressing safety, security, dependability or functionality constraints.

Assessability: Finally, we need mechanisms and tools for assessing and proving the security and dependability of a complex system. Yet, the scale of new ICT systems and the kind of threats and assumptions on their operational environment (not last the human factor) pose new challenges and the need for an assessability discipline is even more impelling. Different metrics, modelling tools and observation mechanisms are needed. The capability of measuring the tolerance to attacks is crucial in new systems that due to their logical and physical diffusion are likely to be under constant attack.

2. Dynamics of Trust.

The lack of trust is one of the main barriers for 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, but also includes the difficulty in modelling trust relationships among digital entities, and between humans and digital entities. Future ICT systems will involve thousands of millions of devices (including nomadic devices), as well as virtual entities (such as Virtual Private Networks and Overlay Networks), and will no longer be able to depend on setting boundaries for their security. Instead, they will require a capability for managing and negotiating trust relationships, adapted to the level of security required in a given situation. The understanding on how trust emerges and evolves as well as of related notions as reputation formation, monitoring and evolution are mandatory. The challenge is then to obtain a greater understanding of partial trust, security-based trust (where trust follows from security), and trust-based security (where security is achieved through a trusted partnership), and to use this understanding to realize a high level of trust of the citizen in the deployment, economic viability and social acceptance of systems and services. This will require expertise and joint research in several fields outside ICT, such as economy and sociology.

3.8.4 Grand Challenge 4. Beyond the Horizon: a new convergence outside the Digital Universe

The **fourth grand challenge** is the preparation of a new convergence at the horizon of 2020 and beyond, which is the *bio-nano-info-quantum "galaxy"*.

Given the economic availability of a new scale of nano-isation and integration, new possibilities of the shape and scope of the global network may emerge. We could observe the decline of the present IP/3G/Google Age by 2010-2015 and we see a disruptive appearance of new infrastructures by 2015. IP may not even survive to the next generation of wireless infrastructures (2015). The 3G will likely be replaced by more open and interoperable infrastructures (2010-2015), and the content galaxy (information, multimedia, programs) will likely be replaced by new services and structures(2015).

During the next twenty years, we may see a long digital twilight and a novel re-emergence of *quasi-analogue* systems with combination of atomic engines (nanotechnology) and/or living cells (organo-geno-technology).

The emergence of organo-nano-infospheres will create a (4D+1D) multidimensional intelligence and disruptive mechanisms for the 21st century. A full new interface security and dependability between those four universes (living + physical + digital + quantum) will have to be devised and developed. The accompanying threats are unenvisageable at this time: some problems such as availability my simply disappear, so long as you can afford the price; others may have solutions resulting from the vast resources that can be deployed by applying nanotechnology, quantum communication and cryptography to tackle security and dependability.

The big question will then be:

> ***how to protect the interfaces, and how to achieve and maintain a security and dependability continuum?***

Convergence of different worlds

We here extrapolate the current trend of technology evolution to forecast TSD challenges of ICT at the end of the next decade.

In the quantum world, technologies appear on the horizon with a focus on photons rather than on electrons. Quantum technologies will need some time in order to compete technically with the silicon and transistor industries, on the one hand, economically with digital technology on the other hand, and in order to seize a specific market. While the digital world has defined seven deterministic layers for communication, to connect a link, to route and transport information and to run applications, it is mandatory for the quantum discipline not only to make reliable communication along direct links, but also to specify what would be the equivalent concepts for information routing and transport. It will be then possible to build quantum networks with applications, which will be complementary to digital networks, probably very different in morphology and size.

By 2010, nanotechnologies and smart dust will be omnipresent. We will be surrounded by invisible autonomous grains (nanotechnology) for which security functions like traceability (tags …), audit, etc. will have to be provided. This era should provide a systemic approach and a federation of standards. But the question remains on how to deal with the various maturities?

In the longer run, by 2020, one can expect digital security to face the wall of Moore's law and make its way into the cracks between the invisible hardware of binary transistors that are proliferating around with malicious attentions, on the one hand, and the scattered host of smart dust software programs, on the other hand. By moving beyond the digital era, we will be reaching the quantum era and we will cross the digital Rubicon, where we would need to address the security of nanotechnologies and bio-computing, by tackling the following issues:

- Quantum Cryptography: upstream research for the distribution of security attributes, using a novel form of trust based on Heisenberg's uncertainty; and, building highly secure quantum networks based on the clear transmission of single photons and/or bundles of photons, able to withstand unauthorized reading thanks to secure protocols based on the observations of quantum mechanics (i.e., the physical impossibility to observe a grain of light surreptitiously without disturbing it and eventually warning the two instigators of quantum communication).
- The security of nanotechnologies: upstream research regarding the marking, on an invisible scale, of the physical world and the trusted infrastructure for the traceability of nanotechnologies.
- The security of intelligent dust: massive passive nano-computers, the future generation of computer swarms, which will be almost invisible and will soon cover our ambient space, label our clothes and accompany the objects of our everyday lives.
- The security of the next convergence on the horizon, the convergence of digital data, and quanta with organo-nano-technologies. In other words there will be a need to trigger a synthesis of the knowledge of the artificial world created from scratch, so as to control the artificial ecosystem which we have been generating for over half a century, to prepare the future creations, to safely explore new territories and to tackle the coming technological disruptions.

The incorporation of virtual and quantum layers in the conventional IT architecture (as shown in Figure 7 – New Planes of the IT architectures), can add other new planes to interact with the other domains such as biology and nanotechnology. These new planes are shown in figure 7.

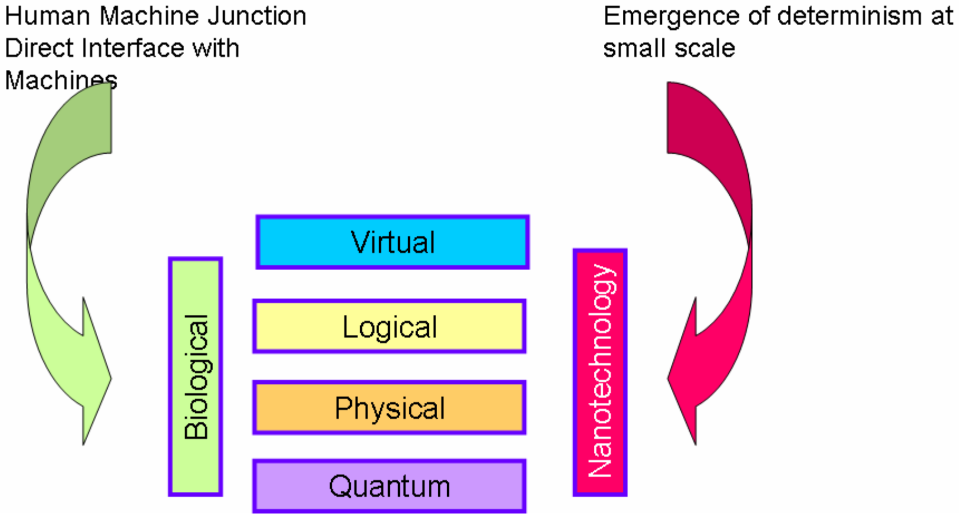


Figure 7 – New Planes of the IT architectures

The next convergence beyond the horizon would be the move of interest to manage complexity as software is no more the innovation engine and with the advent of nanotechnologies there is a return to analogue world. There is an emergence of novel paradigms such as stochastic and quantum paradigms. The future convergence will consist of digital, biology, nanotechnology, and quantum paradigms.

To build a woven Trust from distinct origins and mutual concepts in the digital world, it will be necessary to enhance the universal Shannon models based on the 1s and 0s of texts and the pixels of images. New communication models must be conceived that take into account semantics and aesthetics. These models will combine PKIs, cryptology and steganography in order to enhance, integrate and industrialize digital rights management.

Moreover, Moore's Law would continue its progression until it reached the atomic scale. In ten years the "atomic Rubicon" will be crossed to reach the nanoscopic world. A new era will take shape, that of nanotechnology, which will operate on the atomic level. Computing and networks should then undergo a radical change of nature, since it will be necessary to connect the real world with the invisible.

Nanotechnology and quantum communications after 2010 – a seismic upheaval

Turing's universal computer was the dominant machine of the second half of the twentieth century, and its basic construction has not changed since its creation. The power of computers has doubled every eighteen months, in accordance with Moore's Law, progressing from four thousand transistors in 1970 to a hundred million in 2000. Miniaturization will be followed by techniques enabling finer and finer processing technology. We will soon see the last generation of traditional computers, which will be finger-sized rather than hand-sized, and will become part of the fabric of daily life. Smart tags will replace bar codes, and disposable computers will be inserted in objects, clothes, and under skin. These miniaturized communicating objects, linked to the Internet, will offer a virtually unlimited selection of services. The software on these disposable computers will be accessible from public terminals and managed by devices that have yet to be invented. At this point, we will have pushed transistors to the limits of their atomic scale, but will have entered the age of nanotechnology and traditional computing will make the leap into the quantum age. Nanotechnology will enable the creation of intelligent nanodevices, capable of carrying out specialized tasks. They could, for example be used in a telephone microphone. Quantum cryptography will ensure the transfer of confidential information contained in a new generation of credit cards and SIM cards.

Bio-nano Cyberspace in the Quantum Age around 2020 – a New Era

We can already foresee another convergence that should take place around 2020: that of nanotechnology, biology, quantum communication and traditional computing. This will be the undoing of digital computing as we know it (Shannon's coded data and Turing's coded programs). Hardware, locked in the solitude of Moore's law, will have to break the chains of its obsession with ever finer processing technology. Computing, the prisoner of a double asymptotic curve, consisting of a monotonous dead-end in hardware and inextricable complexity in software, will have to escape the current deadlock if it is to forge the post Internet society.

Computing and Telecom must reconnect with physical reality, returning to the atoms close to silicon in Mendeleev's periodic table (the carbon and hydrogen of living biological cells, indium, germanium, and gallium) and interfacing their peripherals with the human sense organs in order to ensure continuity with our biology. Mathematical modelling and computer simulations will ultimately generate hybrid applications. They will be computers in terms of data processing, but they will also be "real" in the way they will be made up of *in situ* experiences.

The communication personal device of the future is no doubt the first device on this new horizon. Words will be transmitted continuously from our larynx to relay stations and reception may even by-pass the eardrum. This will be a return to the analogue world: computers will draw on various sources, with biological, nano and quantum peripherals. This new world will reduce the Joule effect of circuit heating: computers, telephones and PDAs will have peripherals with motors made up of autonomous atoms, communications and data processing will use quantum states of matter, and bio-computing human-machine interfaces, and the totality will be much less polluting than what we have today.

All the ontologies of this new world, these clusters of living cells linked to a computer, these fleets of nano-robots, and these bundles of photons will be distributed in networks. Some will even be carried within the human body, however, for the time being any representations of this kind environment remain in the realm of science fiction.

4 Conclusions

Our society is rapidly adopting more information and communication technologies (ICT) in private and public services, in commerce and industry, and in the control of the physical infrastructure we rely on. Private information or sensitive data is at increasing risk, and security and reliability problems become significant. Indeed, today people are becoming more and more concerned about the growing complexity of information and communication systems, and the proliferation of privacy-invasive information gathering sources and techniques. In their online daily interactions, they often find themselves faced with high-profile losses or potential disclosure of their personal information with viruses, spy-ware, phishing and other attacks of growing severity and sophistication. As a result, they find themselves in an undesirable situation in which they must put ever more trust into a digital environment in which they have little or no way of understanding, or of assessing the dangers properly.

To build an information society that will deliver growth and prosperity, we need to tailor ICTs to business and social needs, and ensure that they become the foreseen useful tools for economic and social improvement. The starting point for making them useful is to foster trust and to safeguard security in a networked world. In this respect, Europe's research framework programmes are committed to the establishment of a solid security and dependability infrastructure. The IST-SecurIST project was charged with the preparation of a European strategic research agenda in the field of ICT for Security and Dependability, for the upcoming 7th research framework programme (FP7, 2007–2013). To achieve this goal, the project has successfully established two fundamental bodies: the *European Security and Dependability Task Force* (STF), and the *SecurIST Advisory Board*.

The STF comprises over 200 members, spread across thirteen fundamental thematic areas (initiatives) of research, drawn mainly from earlier FP5 and FP6 projects, whose role was to identify thematic based research initiatives Areas, and to identify and to prioritise challenges within Security and Dependability research and development. The STF provided a forum for consolidation and consensus building. The thematic initiatives are shown in Figure 8, which provides a visual interpretation of how these initiatives are integrated and worked together.

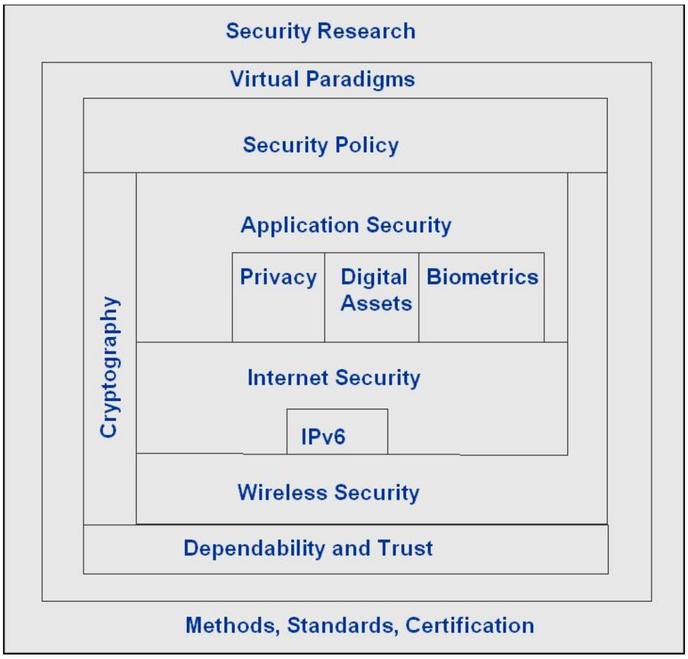


Figure 8 – Outline structure of STF & Initiatives

The SecurIST Advisory Board is composed of European experts in information trust, security and dependability. The charter of the board was to apply their judgement and experience to oversee, review, enhance and promote results from the STF.

A considerable amount of effort went into the formation of the Security Task Force initiatives (Working groups) and the elaboration and consensus of the key challenges from the different constituencies in a large number of workshops and key events. This work was updated since D3.1 Initial Strategy with the inclusion of two important events, Integration workshop of new Unit D4 projects to the STF and the Joint SecurIST Mobile and Wireless Workshop and Security and Dependability held in March 2006 and May 2006, respectively. From the output of the STF [Annex III], there were a number of crucial research areas highlighted:

1. Trust, Security and Dependability (TSD) of new technological infrastructures:
   - IMS, WiMAX networks, ...
   - corporate networks with Voice over IP or multimedia…
   - networks of sensors/actuators with scarce data-processing resources…
   - the Internet of the things [7] (RFiD), protocols of cryptography for devices without contact, cryptography for simplistic data-processing devices.

2. TSD in dynamic ad-hoc networks
   - authentication
   - key management
   - cooperation and fairness
   - secure routing and topology control.

3. TSD for software systems and services:
   - security and dependability of overlay networks, overlay services (dynamic virtual systems), Peer to Peer structures;
   - security of the virtualisation paradigm (horizontal and vertical handovers and associated security, nomadic fast authentications;
   - services in real time, massively distributed, multi-users;
   - management: administration and supervision of these services.

4. TSD of the future Internet :
   - security of post-IP networks in relation to international work (NSF initiatives FIND, GENI) and of the disruptive approaches: security, confidence and impact strength of the future communication networks by integrating their transitions with the current infrastructures;
   - security of B3G infrastructures and the new cellular networks: security of mobility, services and their supervision.

5. protection of critical infrastructures and their interdependences :
   - security and dependability of the wide-area networks and telecommunications systems, of the multi-media services;
   - availability of critical non ICT infrastructures in close connection with the communication networks: modes of help to mitigate breakdowns and the dysfunctions, reduction of potential dominos effects, security policy for crises management, fast deployment of spontaneous infrastructures.

6. infrastructures, protocols and devices for electronic identity (single or multiple) of physical people or entities:
   - new generation device of authentication;
   - digital systems for identities, systems of biometrics;
   - federation of identities, infrastructures and applications with digital signature;

- tools of trust to protect the chains from associated services: personal medical file, identities cards, e-commerce, e-administration;
- secure modules for computers.

7. reinforcement of the protection of private spheres:
    - systems and mechanisms of protection of the private sphere (for an individual, an organization);
    - systems and devices of traceability, follow-up of objects, of guarantee of the property, digital rights management, logistics, invoicing; systems and devices of monitoring, geo-localization of people (for health, parental control) respecting protection of private life and dignity of people.

This deliverable contains the approach taken to date in developing and implementing the ICT Security & Dependability Research Strategy and roadmap beyond 2010. The document outlines the way forward from both the perspectives of the members of the Security and Dependability task force and the SecurIST Advisory board, who have played a pivotal role in reviewing, enhancing, and promoting the work of the STF.

Based on detailed inputs from the STF, the SecurIST Advisory Board issued three versions of reports presenting its recommendations for a future security and dependability research framework in Europe, for the period 2007-2013 [Annex VI]. Version 3.0 takes into account a large number of comments made by the TSD community during an open consultation forum held July – September 2006. Under the headline *From "Security and Dependability by Central Command and Control" to "Security and Dependability by Empowerment"*, the Advisory Board is recommending the following nine key research areas:

1. **Empowerment of the Stakeholders:** User awareness/control in all R&D and ensuing functionality: generic usability, security, trust and dependability;
2. ***Europe-specific*** **Security & Dependability:** Euro-awareness and goals in all R&D and ensuing exploitation;
3. **Infrastructure robustness and availability:** Generic dependability and consistency of all aspects of European (and global) ICT infrastructure;
4. **Interoperability:** Interworking and interoperability of security and dependability across a convergent yet heterogeneous digital world;
5. **Processes for developing Secure and Dependable systems:** Provision and use of trusted tools, processes and procedures to achieve a secure, and dependable digital environment;
6. **Security and Dependability Preservation:** Maintenance of achieved security and dependability states against attack/failure/erosion;
7. **User-centric security and dependability standardisation:** Involvement and consideration of human user needs and sensitivities in development of standards;
8. **Security and dependability of Service Oriented Architectures (SOA):** Establish basics of trust, security and dependability in new Software Systems and Services architectures and approaches;
9. **Technologies for security:** Underlying many of the previous recommendations, relates to ongoing development of existing technologies, and exploration of new possibilities; e.g. cryptology and trusted functionality.

In addition to these nine key research areas, four future *grand challenges* (covering a 10-20 year vision) were compiled. They illustrate possible longer-term possibilities and implications. These are:

1. Countering vulnerabilities and threats within digital urbanization: This challenge addresses open problems that we will face in security and dependability from the expansion and globalization of digital convergence by 2010-2015.
2. Duality between digital privacy and collective security: digital dignity and sovereignty: This challenge deals with future privacy issues of all the stakeholders, whether citizens, groups, enterprises or states. It addresses the problem of how to override the "Big Brother" syndrome and "dark security", i.e., the future assurance of digital sovereignty and dignity for the various stakeholders.
3. Objective and automated processes - *the Reinforcement of the Science and Technical Foundations of TSD*: This challenge addresses the problem of how to attain a controllable and manageable world of complex digital artefacts by 2015 and how to inject regular, quantitative techniques and engineering to make the field truly scientific.
4. Beyond the Horizon: a new convergence – *Going beyond the Digital Universe*: This last challenge deals with the preparation of a new convergence at a horizon of 2020 and beyond, which is the bio-nano-info-quantum "galaxy" and the new security and dependability challenges that will emerge.

The main research topics from the work of the EU Security and Dependability Task Force associated with the nine AB recommendations are summarised, collected and mapped together in Table 2.

Table 2 - Summary of Research Priorities

1. **Empowerment of Stakeholders**	***User awareness in all R&D and ensuing functionality***: generic usability, security, trust and dependability; **Functional requirements**: protection and control/management of all aspects of *identity*, and all aspects of *personal information* and *sensitive data*; trustworthy evolution of systems; usable service-level selection and agreement; mobility & continuity of trust and functionality; usable asset access, transaction, & management; continuous privacy, economic balance and options in services; economic balance and options in engineering; usable human/technology interfaces; personal VPN; protection & management of resources; **Technology requirements:** user-sympathetic cryptology; psychology and physiology of usability; user-sympathetic standardization; legal and regulatory considerations; accountability and forensic considerations; assurance and certification; business models;
2. **Europe-specific Security & Dependability**	***Euro-awareness and goals in all R&D and ensuing exploitation*** **Operational & functional goals:** establish/maintain Euro-leadership in target technologies; establish/maintain Euro-leadership in target services and applications; **Specific technologies**: bio-engineering; cryptology; trusted/assured functionality; human/technology interface;
3. **Infrastructure robustness and availability**	***Generic dependability and consistency of all aspects of European (and global) ICT infrastructure*** **Operational and functional goals:** protection of assets and resources of heterogeneous *and* convergent infrastructure; availability of services, assets and resources; accountability for usage and administration; robust business models and compensation processes; continuity of evolution and migration; dynamic optimal balancing of usability, impregnability, and economics; **Supporting technologies** robust and scalable cryptographic techniques; scalable and manageable availability technologies – redundancy, ubiquity, recovery; trusted/assured functionality; (*via*) trusted development tools and processes (see **Error! Reference source not found.**); new approaches Service Level Agreement, to risk evaluation, and to configuration management;
4. **Interoperability**	***Interworking and interoperability of security and dependability across a convergent yet heterogeneous digital world*** **Operational and functional goals:** transitivity (multi-hop) and transparency (*quasi* single-hop); preservation of security and dependability qualities across and between different technology and administrative domains; protection of privacy and of information; collaborative management, administration, and standards between domains; mutual respect of security parameters and mechanisms; coherence of protection *delivery*, and interpretation of intention and usage; dynamic trust mechanisms and agreements between domains; management of dynamics of evolution and migration; **Supporting technologies** open standards covering policies, semantics, functionality, and interfaces; coherent and compatible tools and processes to deliver trust and assurance; system modelling and mapping;
5. **Processes for developing Secure & Dependable systems**	***Provision and use of trusted tools, processes and procedures to achieve a secure, and dependable digital environment*** **Operational and functional goals:** development of open technical and quality standards; development of {tools & procedures} to enable economic {production, integration, and use} of {verifiable components of a trusted, dependable digital world}; toolkit/workbench delivery & support system; verification/certification

	procedures; delivery, integration and test systems; applicable to system components, service components, applications, add-ons; **Supporting technologies** trusted h/w and s/w environments for *development*, *delivery*, *configuration*, *integration* , *management*, and *operation* of system components; tools and techniques for validation, assessment; verification, certification, and authentication; special protection against attack/subversion; open evaluation criteria, and developmental assurance (eg, to cover open source s/w)
6. **Security and Dependability Preservation**	***Maintenance of achieved security and dependability states against attack/failure/erosion*** **Operational and functional goals** maintenance of integrity of security and dependability of system – and hence of the system as a whole; inherent attack-resistance; specified levels/states as aspect of SLA commitments; monitoring and confirmation services for end-users and for system/service managers and administrators; isolation, repair, and recovery of damaged components (+ trusted disposal); re-certification; damage containment and quarantining; high-trust authorisation and accountability for actions; management of updates, evolution, and migration; **Supporting technologies** open standards, and interoperability; trusted h/w and s/w (OS, particularly) platforms; high-trust diagnosis/test/confirmation tools and techniques; architectural support; integrity checking mechanisms for h/w and s/w; high-trust tools for repair, reconfiguration, and recovery; modelling for damage analysis and management; see 5. above.
7. **User-centric security and dependability standardisation**	***Involvement and consideration of human user needs and sensitivities in development of standards*** **Operational and functional goals** the prominence and priority attached to privacy, identity, and user empowerment issues demand consideration of user needs and expectations at fundamental levels in the formulation of standards (an aspect, itself, of user empowerment); re-think of the roles, rights, and responsibilities of the user; creation and maintenance of trust and confidence, allowing further take up and expansion of the digital world; modelling and exploration of user involvement and usage; fundamental consideration of usability; **Supporting technologies** psychological, physiological, and behaviourist foundations for human perception, use, and interfacing; subjective and objective aspects of trust; legal support – fundamentals (cf Directives) + contractual; establishment of representative bodies;
8. **Security and dependability of Service Oriented Architectures (SOA)**	***Establish basics of trust, dependability and security in new architectures and approaches*** **Operational and functional goals** security and dependability considerations to be included at a fundamental level in new architectural developments; e.g. S&D functionality included in all SOA entities and interfaces, including requirements from above, particularly items3,4,5,&6; + user considerations in items 1&7; **Supporting technologies** again as items 3,4,5,& 6, (plus 1 & 7) above.
9. **Technologies for security**	***Ongoing development of existing technologies, and exploration of new possibilities*** **Operational and functional goals** stronger, faster, smaller, and cheaper developments of current technologies – crypto, silicon, processor design, wireless, opto-electronics, s/w engineering, … ; to be followed – and superseded? – by the new *galaxy*: nano-engineering, quantum computing and cryptography, bio-organic technologies and techniques, that give new meta-Moore orders of magnitude to processing, storage, and communications **Supporting technologies** the two basic techniques are crypto and trusted functionality, including protocols – hence anything and everything pertaining thereto

5 References

[1] Joint M&W Workshop: Security Cluster and D4
http://www.securitytaskforce.org/dmdocuments/sd_cluster.pdf

[2] SecurIST: STF Workshop, January 2005
http://www.securitytaskforce.org/dmdocuments/D2.1_SecurIST_WS1_Report.pdf

[3] SecurIST Workshop in April 2005
http://www.securitytaskforce.org/dmdocuments/D2.2_SecurIST_WS2_Report.pdf

[4] Security Taskforce: http://www.securitytaskforce.eu

[5] SecurIST workshop report March 2006
http://www.securitytaskforce.org/dmdocuments/Microsoft%20Word%20-%20D2.2_Call4WS_reportv3.pdf

[6] SecurIST workshop report, May 2006
http://www.securitytaskforce.org/dmdocuments/jointws_report_v1july0707_reportonly.pdf

[7] www.itu.int/internetofthings

6 Annex I – Advisory Board & Task Force Participation

Table of Contents

6.1 Advisory Board Members

Name	Organisation
Stephan Lechner Chair	Siemens AG
Urs E. Gattiker Vice-Chair	CyTRAP Labs, & CASES Contact
Tobias Christen	Zurich Financial Services
Francois Cosquer	Alcatel
Stephan Engberg	Open Business Innovation
Sonia Heemstra de Groot	Twente Institute for Wireless & Mobile Communications
Bart Preneel	Katholieke Universiteit Leuven
Brian Randell	University of Newcastle
Kai Rannenberg	Goethe University Frankfurt
Michel Riguidel	ENST
Alan Stanley	Information Security Forum
Paulo Verissimo	Faculdade de Ciências da Universidade de Lisboa
Andreas Wespi	IBM, Zurich

Ex-officio members (non-voting) and Administration

Name	Organisation
Jim Clarke	Waterford Institute of Technology
Willie Donnelly	Waterford Institute of Technology
Zeta Dooly	Waterford Institute of Technology
Keith Howker	Vodafone

6.2 EU Security and Dependability Task Force (STF) Initiative Leaders

STF Initiative	Name	Organisation
Application Security Initiative (ASI)	Jim Clarke	Waterford Institute of Technology
Identity and Privacy Initiative (IPI)	Kai Rannenberg	Goethe University Frankfurt
Security Policy Initiative (SPI)	Antonio Lioy	Politecnico di Torino
Security Research Initiative (SRI)	Sathya Rao	Telscom
Dependability and Trust Initiative (DTI)	Paulo Verissimo	FCUL[9]
Wireless Security Initiative (WSI)	Bosco Eduardo Fernandes	Siemens
Biometric Security Initiative (BSI)	Orestes Sánchez-Benavente	Telefónica I+D (TID)
Security Architecture & Virtual Paradigms (SVPI)	Atta Badii	University of Reading
IPv6 Security Initiative (v6SI)	Latif Ladid (co-Chair)	Sub Waterford Institute of Technology
IPv6 Security Initiative (v6SI)	Wolfgang Fritsche (co-Chair)	IABG
Internet Infrastructre Security Initiative (IISI)	Zeta Dooly	Waterford Institute of Technology
Methods, Standards Certification Initiative (MScI)	Alan Husselbee	ISSA (association running the CISSP certification)
Cryptology Research Initiative (CRI)	Bart Preneel	Katholieke Universiteit Leuven
Digital Asset Management Initiative (DAMI)	Mauro Barni	University of Siena
Security Risk Management Initiative (SRMI)	Eyal Adar	ITCON Ltd.

[9] Faculdade de Ciências da Universidade de Lisboa

6.3 STF Membership

6.3.1 ASI Members

Name	Organisation	Contact email
Eyel Adar	ITCON Ltd.	eyal@itcon-ltd.com
Alberto Bianchi	Marconi-Selenia	alberto.bianchi@elsag.it
Oscar Blanco	Ericsson	oscar.blanco@ericsson.com
Jim Clarke	Waterford Institute of Technology	jclarke@tssg.org
William Fitzgerald	Waterford Institute of Technology	wfitzgerald@tssg.org
Gerardo Lamastra	Telecom Italia - TILAB	gerardo.lamastra@tilab.com
Patrick Sinz	Ethiqa SAS	ps@ethiqa.com
Simela Topouzidou	Athens Technology Centre	S.Topouzidou@atc.gr
Konrad Wrona	SAP Labs France	konrad.wrona@sap.com
Pedro Lopez	SGI	plopez@sgi.es
Yannis Kliafas	Athens Technology Centre	Yannis Kliafas@atc.gr
Panos TRIMINTZIOS	Foundation for Research and Technology Hellas Institute of Computer Science	ptrim@ics.forth.gr
Gerard Mannig	Tele2	gerard.mannig@tele2.fr

6.3.2 IISI Members

Name	Organisation	Contact email
Zeta Dooly	Waterford Institute of Technology	zdooly@tssg.org
Eyel Adar	ITCON Ltd.	eyal@itcon-ltd.com
Oronzo Berlen	Getronics	oronzo.berlen@getronics.com
Stephen Butler	LAKE Communications	Stephen.Butler@lakecommunications.com
Latif Ladid	Independent consultant	latif.ladid@village.uunet.lu
Miguel Ponce de Leon	Waterford Institute of Technology	miguelpdl@tssg.org
Patrick Sinz	Ethiqa SAS	ps@ethiqa.com
John Ronan	Waterford Institute of Technology	jronan@tssg.org
Mogens Kuehn Pedersen	CBS, Denmark	mk.inf@cbs.dk
Pedro Lopez	SGI	plopez@sgi.es
Panos TRIMINTZIOS	Foundation for Research and Technology Hellas, Institute of Computer Science	ptrim@ics.forth.gr
Syed Naqvi	CETIC	syed.naqvi@cetic.be

6.3.3 IPI Members

Name	Organisation	Contact email
Kai Rannenberg	Goethe University Frankfurt	Kai.Rannenberg@m-lehrstuhl.de
Kajetan Dolinar	SETCCE	kajetan@setcce.org
Marit Hansen	Independent Centre for Privacy Protection Schleswig-Holstein, Germany	LD10@datenschutzzentrum.de OR prime@datenschutzzentrum.de
Christian Hauser	University of Stuttgart	hauser@ikr.uni-stuttgart.de
David-Olivier Jaquet-Chiffelle	University of Applied Sciences of Bern	david-olivier.jaquet-chiffelle@bfh.ch
Henry Kraseman	Independent Centre for Privacy Protection Schleswig-Holstein, Germany	LD101@datenschutzzentrum.de
Alexandra Michy	SAGEM	alexandra.michy@sagem.com
Martin Neubauer	University of Stuttgart	neubauer@ikr.uni-stuttgart.de
Stefan Weiss	Deloitte and Touche	stefanweiss@deloitte.de
Sven Wohlgemuth	University of Freiburg	wohlgemuth@iig.uni-freiburg.de
Vashek Matyas	Masaryk University in Brno	matyas@fi.muni.cz
Pierangela Samarati	University of Milano	samarati@dti.unimi.it
		ljupcot@tpconsulting.com.mk

6.3.4 SPI Members

Name	Organisation	Contact email
Antonio Lioy	Politecnico di Torino	lioy@polito.it
Tobias Christen	Zurich Financial	tobias.christen@zurich.com
Hervé Debar	France Télécom R&D	herve.debar@francetelecom.com
Ulf Hägglund	Smarticware AB	ulf.hagglund@smarticware.com
Alfred Gottwald	Siemens	alfred.gottwald@siemens.com
Antonio F. Gómez Skarmeta	Universidad de Murcia - Spain	skarmeta@dif.um.es
Konrad Wrona	SAP Labs France	konrad.wrona@sap.com
Panos TRIMINTZIOS	Foundation for Research and Technology Hellas, Institute of Computer Science	ptrim@ics.forth.gr
Pascal Manzano	ENISA	pascal.manzano@enisa.eu.int
Paulo Coelho	Sinfic	pcoelho@sinfic.pt

6.3.5 SRI Members

Name	Organisation	Contact email
Uwe Bendisch	Fraunhofer Institute for Secure Information Technology	Uwe.Bendisch@sit.fraunhofer.de
Anestis Filopoulos	Digitalis Consult	avf@digitalis.gr
Ulrich Friedrich	Atmel	ulrich.friedrich@hno.atmel.com
Mathieu Gorge	VigiTrust	mathieu.gorge@vigitrust.com
Thomas Haeberlen	ENISA - European Network and Information Security Agency	Thomas.HAEBERLEN@cec.eu.int
Michael Kreutzer	Darmstadt University of Technology	kreutzer@dzi.tu-darmstadt.de
Evangelos Markatos	FORTH (Foundation for Research and Technology - Hellas)	"Evangelos Markatos" <markatos@ics.forth.gr>
Tom McCutcheon	Dstl	tgmccutcheon@dstl.gov.uk
Sathya Rao	Telscom	rao@telscom.ch
Mark Reilly	Enterprise Ireland	mark.reilly@enterprise-ireland.com
Reijo Savola	VTT Technical Research Centre of Finland	Reijo.Savola@vtt.fi
Kyriakos Vlachos	University of Patras	kvlachos@ceid.upatras.gr
Michael Kreutzer	TU Darmstadt	kreutzer@dzi.tu-darmstadt.de
Panos Trimintzios	ICS-FORTH	ptrim@ics.forth.gr
Ulrich Friedrich	Atmel Germany	ulrich.friedrich@hno.atmel.com
Quinto Corrado	Lucent Technologies (Belgium)	qcorrado@lucent.com

6.3.6 DTI Members

Name	Organisation	Contact email
Paulo Verissimo	FCUL	pjv@di.fc.ul.pt
Tom Anderson	University of Newcastle upon Tyne	Tom.Anderson@newcastle.ac.uk
Roberto Baldoni	Dipartimento di Informatica e Sistemistica - Univ Roma	baldoni@dis.uniroma1.it
Andrea Bondavalli	Dept : Design and Analysis of Computer Systems - DACS	a.bondavalli@cnuce.cnr.it
Karima Boudaoud	Laboratoire I3S-CNRS	karima.boudaoud@unice.fr
Christian Cachin	IBM Research Zurich	cca@zurich.ibm.com OR cachin@acm.org
Miguel Castro	Microsoft research	castro@lcs.mit.edu
Marc Dacier	Eurecom	marc.dacier@eurecom.fr
Hervé Debar	France Télécom R&D	herve.debar@francetelecom.com
Yves Deswarte	LAAS-CNRS in Toulouse, France.	yves.deswarte@laas.fr
Sofoklis Efremidis	INTRACOM S.A.	sefr@intracom.gr
Nuno Ferreira Neves	Faculdade de Ciências da Universidade de Lisboa	nuno@di.fc.ul.pt
Alfred Gottwald	Siemens	alfred.gottwald@siemens.com
Bernhard Häemmerli	Acris GmbH und HTA Lucerne University of Applied Science	bmhaemmerli@acris.ch
Jörg Kaiser	University of Ulm	kaiser@informatik.uni-ulm.de
Miroslaw Malek	Humboldt-Universität zu Berlin	malek@informatik.hu-berlin.de
Fulvio Marcoz	Finmeccanica	fulvio.marcoz@finmeccanica.it
Refik Molva	Eurecom	Refik.Molva@eurecom.fr
Simin Nadjm-Tehrani	Linköping University	simin@ida.liu.se
Ludovic Pietre-Cambacedes	EDF	ludovic.pietre-cambacedes@edf.fr
David Powell	LAAS-CNRS in Toulouse, France.	david.powell@laas.fr
Brian Randell	University of Newcastle upon Tyne	Brian.Randell@newcastle.ac.uk
Luca Simoncini	Department of Information Engineering-University of Pisa	simon@.iet.unipi.it
Ines Vidal	Euskaltel, S.A.	ividal@euskaltel.es
Konrad Wrona	SAP Labs France	konrad.wrona@sap.com

Neeraj Suri	TU Darmstadt, Dept. of Computer Science	suri@informatik.tu-darmstadt.de
Pedro Lopez	SGI	plopez@sgi.es
Panos TRIMINTZIOS	Foundation for Research and Technology Hellas -Institute of Computer Science	ptrim@ics.forth.gr
Sofía Moreno	AETIC	smoreno@aetic.es
		jlm@lcc.uma.es
Fred Eisner	ABM	fred.eisner@abm.nl
Alexander Romanovsky	NCL	alexander.romanovsky@ncl.ac.uk
Claire Vishik	Intel	claire.vishik@intel.com

6.3.7 WSI Members

Name	Organisation	Contact email
Stephen Butler	LAKE Communications	Stephen.Butler@lakecommunications.com
Daniel Cvrcek	Brno University of Technology	cvrcek@fit.vutbr.cz
Stephan Engberg	Open Business Innovation	stephan.engberg@obivision.com
Thomas Engel	Université du Luxembourg	thomas.engel@uni.lu
Bosco Eduardo Fernandes	Siemens	bosco.fernandes@siemens.com
Antonio F. Gómez Skarmeta	Universidad de Murcia - Spain	skarmeta@dif.um.es
Stephen Hailes	UCL	s.hailes@cs.ucl.ac.uk
Christian Hauser	University of Stuttgart	
Maria Karaguiozova[10]	Infineon Technologies	karaguiozova@polit-data.com
Javier Lopez	UNIVERSITY OF MALAGA	jlm@lcc.uma.es
Anuar Mohd	USM	anuar_mohd@yahoo.com
Erik Norgaard[11]	Atos Origin	erik.norgaard@atosorigin.com>
Mícheál Ó Foghlú	Waterford Institute of Technology	mfoghlu@tssg.org
Riccardo Pascotto	T-Systems International	Riccardo.Pascotto@t-systems.com
Anna Plataki[12]	Infineon Technologies	None given

[10] Registered for SCI, which is now merged with WSI.

[11] Registered for SCI, which is now merged with WSI.

Kyriakos Vlachos	University of Patras	kvlachos@ceid.upatras.gr
Pedro Lopez	SGI	plopez@sgi.es
Panos TRIMINTZIOS	Foundation for Research and Technology Hellas Institute of Computer Science	ptrim@ics.forth.gr
Michael Dieudonne	Agilent Technologies	michael_dieudonne@agilent.com

6.3.8 BSI Members

Name	Organisation	Contact email
Henning Arendt	@bc	ha@atbc.de
Alexandra Michy	SAGEM	alexandra.michy@sagem.com
Erik Norgaard	Atos Origin	erik.norgaard@atosorigin.com
Aljosa Pasic	ATOS Origin	aljosa.pasic@atosorigin.com
Silvia Renteria	ROBOTIKER-TECNALIA	silvia@robotiker.es
Orestes Sánchez-Benavente	Telefónica I+D (TID)	orestes@tid.es
Kush Wadhwa	International Biometric Group (UK)	kwadhwa@biometricgroup.com
Zdenek Riha	Masaryk Univerzity in Brno	zriha@fi.muni.cz
Mark Crosbie	HP	mark.crosbie@hp.com
P. Llobet	TID	Llobet@tid.es
		ha@atbc.de
Raul Sanchez Reillo	UC3M	<rsreillo@ing.uc3m.es>

[12] Registered for SCI, which is now merged with WSI.

6.3.9 SVPI Members

Name	Organisation	Contact email
Atta Badii	University of Reading	atta.badii@reading.ac.uk
Francois Armand	Jaluna	Francois.Armand@jaluna.com
Jerome Billion	Trialog	jerome.billion@trialog.com
Bruno Crispo	Vrije Univeristeit Amsterdam	crispo@cs.vu.nl
Jarkko Holappa	VTT Electronics	Jarkko.Holappa@vtt.fi
Peter Kirstein	University College London	p.kirstein@cs.ucl.ac.uk
Antonio Kung	Trialog	antonio.kung@trialog.com
Alexandra Michy	SAGEM	alexandra.michy@sagem.com
Jan Weber	Omega Management Consultants	omegahighlighter@wxs.nl
Patrick Sinz	Ethiqa SAS	ps@ethiqa.com
Julian Rrushi	University of Milano	julian.rrushi@studenti.unimi.it

6.3.10 V6SI Members

Name	Organisation	Contact email
Latif Ladid	Sub Waterford Institute of Technology	Latif.ladid@village.uunet.lu
Wolfgang Fritsche	IABG	Fritsche@iabg.de
Patrick Cocquet	6WIND	Patrick.cocquet@6wind.com
William Fitzgerald	Waterford Institute of Technology	wfitzgerald@tssg.org
Matthew Ford	British Telecom	Matthew.ford@bt.com
Mícheál Ó Foghlú	Waterford Institute of Technology	mfoghlu@tssg.org

6.3.11 MScI Members

Name	Organisation	Contact email
Alan Husselbee	ISSA (association running the CISSP certification)	ahusselbee@paris.com
Jim Clarke	Waterford IT	jclarke@tssg.org
Bosco Eduardo Fernandes	Siemens	bosco.fernandes@siemens.com
Alan Husselbee	ISSA (association running the CISSP certification)	ahusselbee@paris.com
Sadhbh McCarthy	Local Government Computer Services Board	smccarthy@lgcsb.ie
Tim Willoughby	Local Government Computer Services Board	twilloug@lgcsb.ie
Luc Van den Berghe	CENORM	Van den Berghe Luc" <luc.vandenberghe@cenorm.be>
Ted Humphreys	Chair of IST33 (UK ISO SC27)	Tedxisec@aol.com
Dr. Marijke De Soete	Vice chair ISO SC27	marijke.desoete@pandora.be
Pedro Lopez	SGI	plopez@sgi.es
Laurent.CABIROL	European Commission	Laurent.CABIROL@cec.eu.int

6.3.12 CRI Members

Name	Organisation	Contact email
Bart Preneel	K.U.Leuven (Belgium)	Bart.Preneel@esat.kuleuven.be
Fatih Birinci	TÜBITAK-UEKAE - National Research Institute of Electonics and Cryptology	fatih@uekae.tubitak.gov.tr
Andrew H. Kemp	University of Leeds	A.H.Kemp@leeds.ac.uk
Alexandra Michy	SAGEM	alexandra.michy@sagem.com
Bart Preneel	K.U.Leuven (Belgium)	Bart.Preneel@esat.kuleuven.be
Selçuk Taral	TÜBITAK-UEKAE - National Research Institute of Electonics and Cryptology	staral@uekae.tubitak.gov.tr
Zoltan Kovacs	KRIPTO Research	kovacs.zoltan@kripto.hu
Said Boussakta	School of Electronic and Electrical Engineering, University of Leeds	s.bpussakta@leeds.ac.uk
Jürgen Blum	Cetrel (Luxembourg)	blum@Cetrel.LU

-

6.3.13 DAMI Members

Name	Organisation	Contact email
Mauro Barni	University of Siena	barni@dii.unisi.it
Shay Adar	M-Systems	Shay.Adar@m-systems.com
Omid Aval	Smarticware	omid.aval@smarticware.com
Adrian Waller	Thales Group	Adrian.Waller@thalesgroup.com
Bart Preneel	K.U.Leuven (Belgium)	Bart.Preneel@esat.kuleuven.be

-

6.3.14 SRMI[13] Members

Name	Organisation	Contact email
Eyal Adar	ITCON Ltd.	eyal@itcon-ltd.com
Michel Riguidel	ENST	riguidel@enst.fr
Uwe Beyer	Fraunhofer AIS	uwe.beyer@ais.fraunhofer.de
Simin Nadjm-Tehrani	Linköping University	simin@ida.liu.se
Alan Stanley	ISF	alan.stanley@mac.com
Aljosa Pasic	Atos Origin	aljosa.pasic@atosorigin.com
John Paul Moore	Atos Origin	john-paul.moore@atosorigin.com
Volkmar Lotz	SAP	volkmar.lotz@sap.com
Pascal Bisson	Thales	pascal.bisson@thalesgroup.com
Domenico Salvati	Credit Suisse	salvati@creditsuisse.com
Andreas Wuchner	Novartis	andreas.wuchner@pharma.novartis.com
Louis Marinos	ENISA	Louis.Marinos@enisa.europa.eu
Dr. Haitham Cruickshank	University of Surrey	H.Cruickshank@surrey.ac.uk
Reijo Savola	VTT	Reijo.Savola@vtt.fi
Jim Clarke	Waterford University	jclarke@tssg.org
Bernhard Hämmerli	HTA University	bmhaemmerli@acris.ch
Evangelos Markatos	FORTH (Foundation for Research and Technology - Hellas)	"Evangelos Markatos" <markatos@ics.forth.gr>
Stefan Burschka	Swisscom	Stefan.Burschka@swisscom.com
Tobias Christen	Zurich Financial	tobias.christen@zurich.com

-
-

[13] Security Risk Management Initiative began Sept. 2006

7 Annex II – FP5 and FP6 projects Analysis

7.1 Cryptology Research

7.1.1 FP5 Roadmap: STORK (IST-2002-38273):

STORK (IST-2002-38273) is an FP5 based roadmap project revolving around the area of cryptology. The STORK project was tasked with providing a platform for interchanging ideas and formulating a common research agenda. It has set down a roadmap of open issues in the world of cryptography in the lead up to the FP6 projects [11], [12]. The road map focuses on 4 categories in which it has a number of subcategories to further refine future issues to be solved. These 4 high level categories are:

- Cryptology in the Information Technology Society: eg Digital Wallet
- Cryptographic Protocols: eg. Multiparty protocols
- Cryptographic Techniques: eg. Dedicated attack techniques
- Mathematical Foundations: eg. Information theory

Focusing on the Information Technology Society (IST) area, STORK has highlighted a number of important areas of research.

Network and Mobile System Security Issues:

- Pursue the study of existing security and key distribution protocols such as IPsec, IKE, TLS) to establish formal proofs of security under reasonable attack models.
- Optimized protocols in terms of communication complexity and round-trips.

Digital Wallet, Electronic Cash and Micro-Payments Issues:

- Specify provably secure electronic cash schemes.
- Specify new electronic cash schemes with revocable anonymity.

Ambient Intelligence Issues:

- Design public key infrastructures that can operate in a dynamic, mobile environment.
- Design secure multicast protocols for dynamic ad hoc networks.
- location privacy and anonymity services remain a topic for future research.

Time-stamping Issues:

- The Time-Stamping Authority (based on hash functions) need to be strengthened.
- Time-stamping schemes need to be practical.

E-Voting Issues:

Achieve stronger security notions (non-coercibility, receipt-freeness, etc.)

Digital Rights Management Issues:

- Tamper-resistant software.
- Design better practical fingerprinting schemes with the anonymity factor.
- Find efficient methods to embed fingerprints into the digital content.

7.1.2 FP6: ECRYPT (IST-2002-507932):

ECRYPT (IST-2002-507932) is an FP6 (Network of Excellence) researching the area of cryptology and watermarking [13]. Its objective is to intensify the collaboration of European researchers in cryptology and digital watermarking. Integration of research capabilities is achieved within five virtual labs focused on the following core research areas: symmetric key algorithms (STVL), public key algorithms (AZTEC), protocols (PROVILAB), secure and efficient implementations (VAMPIRE), and watermarking (WAVILA).

STVL basses its research on both the design and analysis of symmetric cryptosystems. Topics covered are:

- Block cipher
- Stream cipher
- Message authentication
- Hash function
- Symmetric cryptographic usability
- Symmetric techniques and their theoretical foundations, including issues such as pseudo-random functions

Within in STVL is a subgroup called *STVL-WG3 a Strategic Research* which is tasked with identifying new problems and areas of research [14]

In February of 2006, the STVL strand of Encrypt has delivered a document outlining ongoing research in symmetric cryptography such as [15]:

- recent proposed algebraic attacks on symmetric primitives
- design criteria for symmetric ciphers
- provable properties of symmetric primitives
- major industrial needs in the area of symmetric cryptography

As a result of investigating these current trends, the STVL group has identified 4 critical areas of future research:

- A need for lightweight algorithms (especially for low-cost stream ciphers), dedicated to hardware environments where the available resources are heavily restricted, arises from industry.
- Attacks on different commonly used hash functions must be further investigated. Hence the development of new general design principles for hash functions (and for MAC algorithms) is a major challenge
- There is a need to better understand the principles and techniques of recent algebraic attacks which may threaten both stream and block ciphers.
- The development of new cryptanalytic techniques, such as algebraic attacks, has important consequences on the properties required for the elementary functions used in a symmetric cipher. Therefore, there is a need for a clarification of all design criteria which must be prescribed for a given application.

AZTEC researches the design and analysis of asymmetric cryptographic techniques. Topics investigated in this virtual lab are [16]:

- Asymmetric encryption or public-key encryption

- Digital signatures
- Techniques for asymmetric cryptanalysis

A major factor with the AZTEC strand of ECRYPT is provable security. Provable security is an attempt to formally define security for asymmetric cryptographic problems [17].

PROVILAB coordinates research in cryptographic protocols and has categorised protocols as:

- Two-Party Protocols
- Multiparty Protocols
- Unconditionally Secure Protocols

There are 3 finalised deliverables that define the state-of-the-art of each of those categories above and it also lists some technical open issues [18], [19] and [20] . For example in [18] zero knowledge proof systems and oblivious transfer issues are raised.

Such protocols involve interaction between two or more agents, who can be humans or machines. The goal of a protocol can be of technical nature, such as agreeing on a secret key for subsequent secure communication, secure identification of agents or reliable broadcast. But the goal can also be of more application-oriented nature, such as secure payment systems, fair exchange of information, secure electronic voting or secure auctions and contract bidding. Secure protocols must reach their goals despite attacks, even from agents who participate in the protocol.

VAMPIRE is researching the development of novel efficient implementation techniques in hardware and software cryptography along with the gaining experience in understanding existing and new side channel attacks. This research group is divided into 4 distinct areas:

- Software Implementation
- Hardware Implementation
- Side-channel Attacks
- Strategic Research

VAMPIRE has to date produced documentation that details hardware architectures state-of-the-art [21] and its corresponding hardware algorithms [22]. The group has also address areas of cryptographic attacks in particular electromagnetic fault attacks [22] and hardware crackers [23].

WAVILA is investigating watermarking, perceptual hashing, domain embedded signalling and fuzzy signatures. It has expectations to be able to utilise these aspects in areas of digital rights management and mpeg-21. The group highlights due to watermarking immaturity the wide scale adoption is not happening and hence there is a need to investigate it more in the future tot make it a more mature area.

This strand of ECRYPT has delivered numerous documentation to describe the fundamental principles of watermarking, practical systems, forensics, benchmarking tools and so forth [24], [25], [26] and [27].

ECRYPT as a whole has built upon the FP5 cryptography roadmap in that it has researched the area of multi-party protocols, dedicated attack issues and so forth.

7.1.3 FP6: SECOQC (IST-506813)

The SECOQC (Development of a Global Network for Secure Communication based on Quantum Cryptography) is an FP6 project that aims at developing novel key distribution solutions in the area of quantum cryptography.

The research objectives and challenges that SECOQC aims to address are to [63]:

- Develop fully functional Quantum Key Distribution (QKD) devices. These would realise a QKD primitive i.e. continual generation of renewed identical keys on demand at two distinct locations (e.g. secure centres) situated at short to medium range distances;
- Develop a novel security architecture by designing abstract-level cryptographic protocols, which allow secure long-range communication on the basis of the highly secure QKD primitive;
- Design a suitable QKD based network architecture and create an initial experimental implementation;
- Evaluate the capacities of this experimental system for network security;
- Finally, in the perspective of the future internet economy and post third generation telephony, evaluate the economic interest of this new secure network infrastructure that facilitates the sharing of secret information.

7.1.4 FP6: TIRAMISU (IST-506983):

The Innovative Rights and Access Management Inter-platform SolUtion (TIRAMISU) is an FP6 project that aims to develop a complete end-to-end multimedia framework that will enable the creation, delivery and use of digital media content on the public network, while protecting the rights of content owners and the privacy of consumers. The project shall focus its attention on a standards-based Digital Rights Management (DRM) system that maintains a reasonable balance between end-user expectations and the rights preservation of the content owners [42].

This section only details the research and challenges highlighted by the project in terms of digital rights management.

TIRAMISU notes that despite the large body of research devoted to DRM and its integration into existing distribution channels the level of adoption has been inadequate, especially when Internet and P2P distribution are considered. From an end-user’s perspective, DRM solutions are usually perceived as both obtrusive and restrictive. Complex purchase procedures, restrictions in copying content for personal backups and use on other devices the user may own has contributed to this [42].

Three high level business based requirements that are currently under investigation and still ongoing are:

- **Efficient Use Control:** Prevent illegal use of the protected media.
- **Motivating Obedience:** respect user rights and pay royalties but also to protect consumer privacy.
- **Law Enforcing Assistance:** Enable tracing the media source and trail and make it difficult for violators to stay anonymous.

To combat the above business requirements, lower level technological challenges need to be met. The project has divided these challenges into 13 categories:

Security

- Media shall be stored and delivered in an encrypted format that prevents illegal access.
- Keys will only be distributed to authenticated rights holders only.

- The media handling program shall not divert the use of the descrambling key for a purpose other than the one expressed in the license.
- The key shall be used in automated operations only. The key will not be available to the users.
- The DRM system should be strongly resistant to tampering.

7.1.4.1

Monitoring

- Monitoring will be used to force royalty payment according to license terms and to enable automated levy collection.
- Report of such events and violations to management systems.

Closing loopholes

- Protect the media from creation phase to consumption phase in such away that the media is never found in unencrypted form at any intermediately phase
- Provide strong key safes and prevent a key being used for operations that are not allowed by the license terms.

Interoperability

- provide a standard algorithm to scramble the media.
- provide standard signaling.
- provide a standard environment for key management.

Impersonation

There is a need for impersonation that is an association between licenses and virtual identities:

- The license holder shall be authenticated through a virtual identity (VI)
- The VI should be easily transferred between devices supporting such impersonation.
- The VI should maintain the anonymity of its owner.
- It should be easy to transfer licenses between VIs.
- The VI should be compatible with all devices.
- It shall be very difficult and/or expensive to replicate a VI without authorization.
- It should be possible to recover a VI after loss or damage.

Versatility

- Protected items need be able to travel through heterogeneous networks and be stored securely.
- The DRM system needs to support scalable media coding without hindering the full potential of that technology.

Accessibility

- Once license is obtained and applied, no further manual operation is required in order to access the media.

- Unless specifically restricted by the license terms, media should be accessible in all environments (in house, on the road etc.) and in all geographic locations, as long as a consuming device is available.

Non-Restrictiveness

- Personal backups should be allowed.
- Recording excerpts for personal use.
- Lending media items to friends.
- Selling used media.

Simplicity

- Avoid adding complexity to the consumers.
- Simple mechanisms for license trade.
- Simple mechanisms for enabling the licenses on devices.
- Simple payment and subscription methods.

Affordability

- The cost DRM capabilities protecting the content is proportional to the financial gains of content protection.

Privacy

- Both media and licensing should be delivered to the customer while preserving the customers privacy.

Identification

- Persistent association of details about the source of the media and rights ownership.
- Persistent association of general licensing terms (e.g. protected/ unprotected).
- Association between the media item and references for acquiring a license to peruse it.

Traceability

- It is difficult to find and prosecute the violators so:
- It should be difficult to illegally copy media without leaving fingerprints.
- It should be difficult to distribute pirated media anonymously.
- It should be difficult to consume pirated media anonymously.

7.1.5 FP5: CERTIMARK (IST-1999-10987)

Certification of Watermark Techniques (CERTIMARK) was an FP5 project that designed a benchmarking suite for still picture and video watermarking technologies.

The project highlights that the then current state-of-the-art watermarking schemes had been introduced to improve the visual imperceptibility of watermarks in images and their robustness to attacks from users. However there was still a lack of a universally recognised procedure enabling comparisons of their performances resorting to common and objective criteria with respect to existing (and future) applications [44].

The aim of CERTIMARK project is to define and develop an objective benchmark comparison of characteristics of watermarks tool. It follows two tracks to accomplish this task:

- A list of key parameters that should be taken into account in CERTIMARK benchmarking metrics and methodology as they are considered as important for user applications (deliverable 2.2).
- Specific usage scenarios that are of interest to CERTIMARK and the real world (deliverable 3.1).

Several business watermarking application fields where identified [44]:

- **Proof of Ownership over an Image - "Robust" Watermarking:** the detection of the mark with a private key or the hidden message itself helps in proving the ownership on a document.
- **Monitoring of the Exploitation of Broadcast or Distributed Images:** monitoring globally corresponds to tracing the distribution of some images on a given media of distribution. So, it concerns the evaluation of broadcast audience of a programme (also called: people metering) in a legal context, as well as the tracking of piracy (illegal exploitation) of some creations on a distribution media. But, its aim only remains detection of the exploitation of images.
- **Fingerprinting:** in order to complete the tracing of image exploitation on a distribution media, a different mark is inserted in each distributed copy of an image before delivery by its legal distributor. This identifies a transaction or a sold item.
- **Document Integrity** Checking - "Fragile" Watermarking: the mark permits to detect eventual changes in an image due to some attacks and their locations. Then, it is expected to be partly alterable.
- **Authentication and Identification of an Image:** a user which receives an image may need to identify the source of a document or the document itself with a high degree of certainty, in order to validate this document for a specific use.
- **Usage Control:** the reception of some distributed images by some digital equipment in a distribution network, may be controlled in using watermarks inserted in these images, and only enabled on equipment whose owner paid some access rights. A first example of it is provided Copy Protection on DVD & CDROM for the Consumer Market a mark is embedded in DVD video disks in order to prevent copy of DVD, in co-operation with playback and recording devices manufacturers.
- **Information Side Channel:** this is globally related to "conveying" side information. About carrying public or private information, we generally think of information which is related to the image creation, and which is made available or not, to any receiver (depending on its nature). At the opposite, Steganography is concerned with secretly carrying information that has nothing to do with the "cover" image: this really constitutes a separate channel.

7.2 Identity Management & Privacy Research

7.2.1 FP5 Roadmap: RAPID (IST-2001-38310):

Roadmap for Advanced Research in Privacy and Identity Management (RAPID) was a FP5 project (IST-2001-38310) that identified research topics in the area of Privacy and Identity Management [28]. RAPID derived its results from address the following 5 areas:

- Privacy enhancing technologies (PET) in infrastructures
- Privacy and Identity Management (PIM) in enterprise systems
- Multiple and dependable identity management

- Legal PIM issues
- Socio-economic PIM issues.

The RAPID roadmap introduces three potential scenarios for its vision of PIM in society:

- “Positive”: Identity Management integrated with Privacy Protection adds value for users, business and government. This means that PIM is becoming more and more important, policy makers address PIM in new regulations, users need new PIM products to meet their needs, etc.
- “Steady state”: Identity Management and Privacy Protection are two separate things. The privacy protection arena is for special niche markets with a strong battle between Law Enforcement and Privacy Protection. PIM will grow slowly in special markets and delivers only a baseline protection.
- “Negative”: Users are not interested in Identity Management and Privacy Protection. Users expect active use of their profiles by business and government for value added and cheaper services. PIM is becoming less important, PIM regulation will be stripped, users lose interest in privacy.

RAPID roadmap focuses on the positive scenario because it believed that scenario faced the most important of research challenges. The project has defined research challenges under the following areas technical challenges and non-technical challenges.

7.2.1.1 Technical Challenges:

Multiple & Dependable Identity Management:

This covers the area of dependable and multiple identity management systems for individuals who need to exhibit different online roles (employee, partner, customer, etc.) within different societal and technical contexts.

Priority areas defined in the roadmap are:

- Provisioning, revocation, profile management of identities and prevention of identity proliferation.
- Development of user-side architectures and interfaces for identity management and privacy preference management.
- Integration of these architectures with server-side systems and with mechanisms for access control to resources.
- Secure user devices allowing for privacy friendly access control based on user profiles and preferences.
- Dependable defence-in-depth identity protection technologies to prevent identity theft.
- Tools for end users to control secondary use and linkability of partial identities.

Infrastructure:

The RAPID project understood that anonymity functionality has an important role in a variety of interactions in society and helps to protect privacy. Hence different classes of anonymity functions have been introduced roughly aligned to the various communications layers: Address Privacy, Location Privacy, Service Access Privacy and Authorisation Privacy.

Infrastructure future research areas are:

- Address privacy: care attention needs to be placed with regard to linkages to a users habits via IP address monitoring.

- Location privacy: a need for user controlled mechanisms to avoid or in some cases consent to location based devices or protocols.
- Service-level Privacy: provide anonymous/pseudonymous services.
- Authorisation Privacy: Non-identifying authorisation schemes.

Enterprise Identity Management:

This involves the authentication of the user, if required, in a non-identifiable way, and then determines what the user can do with information resources while it protects the enterprise information and alerts the enterprise if this information has been compromised.

Identified research challenges for enterprise service systems:

- Enterprise systems PET functions: Privacy access control and anonymity provision.
- Enforcement technology: violation detection schemes.
- Ontologies and authorisation policies.

7.2.1.2

7.2.1.3 Non-Technical Challenges:

Socio-Economic:

This area focuses on how privacy and identity management issues can effectively be dealt. What are its impacts in a commercial environment.

The socio-economic research challenges are:

- Privacy classification in Europe for the citizen.
- Analysis of the PIM toward the digital identity service industry.
- Analysis of the PIM relation towards the Government to citizens and enterprises.
- Analysis of the ways and conditions to raise awareness for ICT users.
- Analysis of the ways and conditions to stimulate PIM producers and development of PIM Business models.

Legal:

Develop a to bridge the gap between technology and regulation.

Research challenges for legal topics comprise:

- Privacy ontologies: translating legal clauses into machine-readable policies.
- Multiple digital identities: legal implications of concepts of online identities.
- Legal implications of use of online anonymity and pseudonymity.
- Legal boundaries of privacy friendly concepts of Public Key Infrastructures.
- Legal boundaries of privacy friendly Digital Rights Management.
- Privacy requirements vs. the need for functionality in E-government.
- State security and law enforcement.

7.2.2 FP6: FIDIS (IST-2002-507512):

Future of Identity in the Information Society (FIDIS) (IST-2002-507512) is an FP6 project that is researching how appropriate identities and identity management can progress the way to a fair(er) European information society [29].

The project is divided into 7 research activities[14]:

- "Identity of Identity"
- Profiling
- Interoperability of IDs and ID management systems
- Forensic Implications
- De-Identification
- High-Tech IDs
- Mobility and Identity

FIDIS has delivered a number of deliverables strategically defining its current knowledge and expectations on where identity management is heading most notably:

- D3.1 Overview on Identity Management Systems
- D3.2 A Study on PKI and Biometrics
- D3.3 Study on Mobile Identity Management
- D4.2: Set of Requirements for Interoperability of Identity Management Systems
- D6.1Forensic Implications of Identity Management Systems
- D7.3 Report on Actual and Possible Profiling Techniques in the Field of Ambient Intelligence
- D7.4 Implications of Profiling Practices on Democracy

The following is just a brief overview of the relevant deliverables in relation to where identity and privacy based management needs to further develop and its linkages of the RAPID and BioVision roadmaps.

The “D3.1: Overview on IMS” deliverable details an overview of existing identity management systems (IMS). Privacy enhancing mechanisms are elaborated and selected corresponding privacy enhancing technologies (PET) are shown as examples of existing implementations of those mechanisms. This project has investigated over 60 different IMS technologies and approaches such as “Liberty Alliance” [30]. FIDIS has taken the research of PETs outlined by the FP6 RAPID roadmap to a deeper level of understanding and as a result has categorised IMS into 3 categories:

- Type 1: IMS for account management, implementing authentication, authorisation, and accounting,
- Type 2: IMS for profiling of user data by an organisation, e.g. detailed log files or data warehouses which support e.g., personalised services or the analysis of customer behaviour,
- Type 3: IMS for user-controlled context-dependent role and pseudonym management.

[14] Further research activities begin in the third workplan of the project (2006-2009).

As a result of above mentioned deliverable the research has returned with some research challenges still to be addressed in the future:

- The perception differs widely of what identity management is. Hence a clearer taxonomy and public awareness are necessary.
- Integration of the existing, technologically feasible solutions is generally poor and hence interoperability therefore a major area of interest.
- There is a large requirement for integrating good usability features.

The D3.2 deliverable is a comprehensive study on PKI and biometrics, specifically from the legal and technological point of view, with focus put on the possibility of privacy-enhancing implementations [31]. Its researches ways to improve the diffusion of electronic signatures into European markets six concrete measures:

- To shift costs in order to achieve a fair distribution
- Measures to reach the critical mass of users
- Increasing awareness and knowledge about this technology
- To especially target the user group called 'early adopters'
- To increase triability e.g. by trial versions of electronic signatures
- To further reduce complexity of the needed private infrastructure

FIDIS researches some of the challenges set out in the BioVision roadmap towards biometric security and its relationship with privacy management. From a technological and economic perspective all biometric methods used today for authentication and verification depend on the following 3 factors:

- Quality (low False Acceptance Rates (FAR), secure systems with e.g. high tamper resistance and compliance to the privacy criteria of the European Art. 29 Data Protection Working Party (WP 29))
- Convenience (easy and quick enrolment, use and maintenance, low False Rejection Rate (FRR))
- Costs for the needed infrastructure

The D3.2 deliverable researches technological weaknesses with respect to quality and convenience of the biometric methods. It notes that one method of biometric capture does not fit all people for example: iris recognition doesn't work with people having aniridia or genetic fingerprinting issues with monozygotic twins.

This deliverable notes the following as a research challenges with respect to implementation of privacy criteria are still open from the perspective of currently available solutions. In some cases it is not known whether privacy-critical information e.g., concerning health, can be extracted from templates. This is notably not thoroughly investigated in areas where numerous different algorithms are used to generate templates, e.g. for face recognition. Further research is necessary in this area, however it is expected that this will not be driven by the economic sector due to the lack of economic interest. D3.2 also notes a similar future challenge like the BioSec project in delivering highly dependable "liveness" detection systems.

FIDIS also addresses the issues of mobility of identities (D3.3) and strategic measures to build upon now and into the future. The deliverable states that mobile identity is in its infancy. For example, GSM networks provide with the management of SIM identities a kind of mobile identity management, but they do not realise all requirements for mobile identity management. Unlike the static identity already implemented in current mobile networks, dynamic aspects, like the user's position or the temporal context, increasingly gain importance for new kinds of mobile applications.

The project has highlighted new security threats such as a mobile user's location information and their personal preferences for the configuration of their mobile device's user interface. Hence there is still a lot of research to be done in this area.

D3.3 has also raised another area of future research in that not only is privacy important but usability of mobile identity management systems is relevant for the success of mobile identity management, too. Usability influences the correctness of security mechanisms. Since being secure is not a primary goal of users and since they do not want to learn the respective security mechanisms, mobile identity management has to be comprehensible for security for the everyday user.

7.2.3 FP6: PRIME (IST-2002-507591):

PRIME (IST-2002-507591) elaborates a framework to integrate all technical and non-technical aspects of privacy-enhancing Identity Management (IDM). Its aim is to advance the state of the art to address foundational technologies (human-computer interface, ontologies, authorization, cryptology), assurance and trust, and architectures. It validates its results with prototypes and experiments with end-users, taking into account legacy applications and interoperability with existing and emerging IDM standards.

PRIME describes the environment within Europe which on the one hand is characterized by slow erosion of citizen privacy by large corporate industries and government agencies. Fortunately there Europe has an elaborate legal framework aimed at protecting personal citizen data. This framework sets the conditions for the processing of personal data, and offers individuals the right to inspect the data held on them by organisations processing personal data, as well as the right to have errors corrected, and data removed from certain databases [33]. However, these legal framework is limited at best and its PRIMES goal to facilitate citizens with information services in a reliable and trustworthy way while keeping sovereignty over their private sphere under the same or better conditions that they are offered in the paper-based world.

In its Framework deliverables and the annual research reports, PRIME currently highlighted several challenges for future research [34, 35, 48, 49]:

- User-informed consent and control: keep control what quantity of personal data is given to whom and for which purpose. Hence a user-controlled identity management system needs to be constructed to allow the stakeholders concerned and the interacting technologies to address privacy issues.
- Privacy negotiation, agreement and dispute handling: The vision enables users to express their privacy policy and preferences, stating how and under which conditions their personal data may be handled by others outside the private sphere.
- Data minimisation and identity management: disclosure of personal data is on a need-to-know basis only.
- Accountability: provision of pseudonym technologies.

7.2.4 FP6: CONNECT (IST-026464)

CONNECT is an FP6 project that aims to implement a privacy management platform within pervasive mobile services. This research will involve coupling research on semantic technologies and intelligent agents with wireless communications (including UMTS, Wi-Fi and WIMAX), context-sensitive paradigms and multimodal (voice/graphics) interfaces to provide a secure framework to ensure that privacy is a feasible and desirable component of future ambient intelligence applications [23].

Context-aware mobile services are set to rise in the future: current applications range from car navigation systems, to buddy services that inform users when a friend is nearby, to location-based advertisements, which marketers send to users on the basis of their current position. Such applications raise serious privacy issues that must be addressed both to appease public concern and to comply with current legislation such as the recent 2002/58/EC directive which requires the explicit consensus for the use of privacy sensitive location.

CONNECT's research objective will be to satisfy users' needs to control their context/location privacy and contemporarily the need to minimise the demands made of user interaction for privacy authorisation in order to make happen Ambient Intelligence's view of pervasive technology.

7.3 Dependable & Critical Infrastructure Research

There were a number of roadmap projects within this area of research including Accompanying Measure System Dependability (AMSD), Active Loss Prevention for ICT eNabled Enterprise (ALPINE), Dependability Development Support Initiative (DDSI), and the Analysis and Assessment for Critical Infrastructure protection (ACIP).

7.3.1 FP5 Roadmap: AMSD (IST-2001-37553):

Accompanying Measure System Dependability (AMSD) was a FP5 project that delivered a dependability roadmap that considered dependability in an adequately holistic way, and a detailed roadmap for dependable embedded systems. Dependability was addressed in terms of reliability, safety, survivability, security, privacy & identity management, embedded systems, mobile privacy and security smart cards, biometrics, cryptography, protection of critical infrastructures, and dependability policy [36]. The AMSD project has interoperated and learned from the knowledge of other FP5 projects when it delivered its final roadmap for dependability [38].

Future system interactions and interconnections will raise complexity issues and future research should involve dependability analysis and dependability techniques. AMSD has highlighted six key categories of research [37]:

- **Evolution & Dynamics**: To understand, evaluate and predict the behaviour of large dynamic (AmI) socio-technical systems of systems (c1-c4, c10, c25-c26).
- **Design, Development & Evaluation:** To be able to design, develop, evaluate and deploy cost-effective systems and components that are adequately dependable (c5-c10).
- **Meta-data**: To understand, design, develop, evaluate and deploy meta-knowledge and meta-data (c11-c14).
- **New Threats & Vulnerabilities**: To understand, evaluate and predict, and provide means for dealing with new threats and vulnerabilities (c15-c17).
- **Risk Issues:** To be able to understand, evaluate, communicate, control, remove and mitigate the risks associated with the AmI vision (c18-c25).
- **Multi-Disciplinary Approach**: The need for a multi-disciplinary (and where possible an interdisciplinary) approach to the technical issues, and to the socioeconomic, industrial and policy aspects (c25- c26).

With these six key areas the projects has defined 26 core challenges of the future [37]:

- **c1**: “Ability to evaluate and predict the dependability of systems that change, or whose dependability requirements evolve, and to design and develop systems that can cope with those changes”.
- **c2:** “Ability to evaluate and predict the dependability of systems located in dynamic settings, and to design and develop systems that can cope with these dynamics”.
- **c3**: “Ability to develop dynamic dependability cases that can tradeoff contradicting properties and to address correct/complete information fusion and uncertainties on the correctness of the ambient data”.
- **c4**: “Ability to understand and exploit the dynamics between the evolution of offensive and defensive measures in the design, development and upgrading of systems (the dependability “arms race”)”.
- **c5**: “Ability to design, develop and deploy systems with user perceived qualities of trustworthy, discreet, aware, autonomous, responsible, timely, replaceable, resourceful, loyal and mobile”.
- **c6**: “Ability to understand the personal relationships between people and technological artefacts so as to predict and ameliorate any new pathologies”.
- **c7**: “Ability to translate user views of QoS into service attributes and these into component requirements”.
- **c8**: “Ability to define the required dependability and evaluate the achieved reliability of complex non-deterministic speech recognition, visualisation and learning systems”.
- **c9**: “Ability to develop, evaluate and deploy ultra-critical components for networked ambients”.
- **c10**: “Ability to evaluate dependability of large complex systems that have to be analysed as aggregation of subsystems”.
- **c11**: “Ability to deal with dependability of meta-data especially how to describe and articulate the level of trust that can be put in knowledge”.
- **c12**: “Ability to have intuitive and undemanding ways for expressing, verifying and modifying meta-information that are central to a system dependability and trustworthiness, such as policies and preferences of individual and groups”.
- **c13:** “Ability to link agent actions to potential risks, and to provide appropriate means to all stakeholders to manage them”.
- **c14**: “Ability to assure with the dependable functioning of heterogeneous agent based systems, where the agents can represent humans”.
- **c15**: “Ability to ensure that the (commercial, social) advantages of data aggregation and mining do not violate personal or business rights, or valid user preferences, or legal provisions”.
- **c16**: “Ability to establish accountability for actions while maintaining privacy and business confidentiality in a distributed, dynamic environment”.
- **c17**: “Theories, methods and tools to assess the dependability consequences of interactions and coupling from shared computational resources”.
- **c18**: “Ability to characterise required and achieved dependability in appropriate terms and to link them to the dependability characteristics of the underlying services”.

- **c19**: "Methods to establish a dynamic, socially variable tolerability of risk. To understand how trust and confidence is won, maintained and lost taking into account factors such as the social dynamics of risk".
- **c20**: "Ability for users to being aware of the implications of the use of systems, characterize the consequent delegation of responsibility, set limits, change and monitor this delegation".
- **c21**: Ability to assess the causes and consequences of failure propagation by cascading and escalation and corresponding methods for describing the required dependability attributes(robustness, resilience, survivability...)
- **c22**: "Ability to design and implement data collection and sharing systems (including technical, legal and contractual aspects), on an international basis, for diagnosis of incidents, forensic activities and learning from experience".
- **c23**: "Ability to ensure the risk management and governance of any systemic consequences of failures of the information infrastructure; that society-relevant risks are identified and evaluated; and that the limitations of the market and other mechanisms are understood and addressed".
- **c24**: "Multidisciplinary approach for the evaluation and communication of risk and benefits of AmI scenarios".
- **c25**: "Ability to model and understand the human/technical/ social/market interactions in dependability analysis and in developing dependability techniques".
- **c26**: "Ability to consider the policy, social, economic and industrial context for the deployment of dependability solutions".

7.3.2 FP5 Roadmap: The ALPINE Project

The ALPINE (Active Loss Prevention for ICT eNabled Enterprise) was based on a multi-disciplinary approach to managing risk and establishing secure e-Business transactions based on paradigms already well-established to protect other business activities and investments. These well-established techniques for protecting investments can be applied to e-Business through a collaborative approach amongst the key professional disciplines of legal, audit, insurance, accounting, commercial, technology, and regulation.

The ALPINE project partners have completed a 7 project deliverables, of which 5 were developed in Special Interest Groups led by a designated partner, and 2 were additional deliverables from The Open Group:

- ESI - Security Policy Management for Small & Medium Enterprises SIG
- ETIS - Liability in Mobile Transactions SIG
- The Open Group - Trust Services Mapping SIG
- ESI - Trustmarks
- The Open Group - Dependable Embedded Systems
- The Ope3n Group - Market Study
- The Open Group - Roadmap for Further Research

7.3.3 FP5 Roadmap: Dependability Development Support Initiative (DDSI)

The Dependability Development Support Initiative (DDSI), an EU-supported Information Society Technologies project which ran between June 2001 and November 2002, aimed at supporting the development of dependability policies across Europe and across sectoral boundaries by:

- Establishing networks of interest among the leading European and international stakeholders (European institutions, national governments, industry and civil society)
- Providing baseline data about dependability initiatives around the world
- Preparing policy roadmaps targeted at industry, national governments and European institutions.

The emergence of an Information Society in Europe has led to a growing recognition of the need to ensure an environment in which dependable and trustworthy information infrastructures can be developed. As Europe becomes more dependent upon electronic communications and information exchanges, so critical business and social processes become more vulnerable to accidental or malicious failures of IT systems and networks. But, building a safe and secure Information Society requires more than technology. Comprehensive policy initiatives at the European level are required to help protect citizens, support business and secure critical infrastructures.

While no specific technological based projects could be mapped directly to this roadmap project in Figure 1, since some of the technological findings from the project were more than likely addressed within AMSD, we decided to include this roadmap project also under the area of DCI.

7.3.4 FP5 Roadmap: ACIP (IST-2001- 37257):

The goal of ACIP was to provide a roadmap for the development and application of modelling and simulation, gaming and further adequate methodologies and tools for the following purposes:

- identification and evaluation of the state of the art of critical infrastructure protection (CIP);
- analysis of mutual dependencies of infrastructures and cascading effects in case of disturbances;
- investigation of different scenarios in order to determine gaps, deficiencies, and robustness of CIS;
- identification of technological development and necessary protective measures with respect to CIP.

The project initiated dialogues with industry, academia, public authorities, and other users as well as providers of infrastructure, to seize R&D needs, and R&D resources as well as threat perception, vulnerabilities and related preventive measures. Stakeholders will be invited to discuss the results and to contribute to the work in progress in workshops and to co-ordinate and co-operate with other ongoing or planned initiatives and programmes related to CIP.

7.3.5 FP6: SEINIT (IST-2002-001929)

SEINIT (IST-2002-001929) was an FP6 project that researched various security elements to ensure a trusted and dependable security framework that was ubiquitous, that utilised heterogeneous networks, with focus on the ambient intelligence around an end-user. The framework was also organisation neutral. The technological objectives were to design, and then develop the components to be implemented, to integrate existing and new components on security assessment platforms capable of running real life scenarios. The project developed new security models the address current challenges and built the architecture along with its components to address the nomadic, pervasive, multi-players communicating world. The research focused on the availability of IPv6 networks and dealt with the usage of such networks as well as co-existence of IPv4 and IPv6 equipment and sub-networks [70].

While SEINIT addressed its research focus (threats analysis, security audits, specific security issues of ambient intelligence, network infrastructure, mobility and security;, monitoring mechanism, interdependence of QoS, accounting and security in emerging converged networks, law enforcement and privacy) it was able to define future security threats within networks and the internet [71]:

- The end of Moore's Law. Moore's Law (the speed and memory of a computer doubles every 2 years) will end its long life, seeing that the present technology will reach its full capacity in a short time.
- The digital world will become increasingly mobile and interconnected. It will soon be impossible for a company to protect only the entry points in its network, given the ease of hackers to connect to the network itself.
- Smart labels (RFID) are appearing on the horizon, replacing barcodes and other types of product identification.
- New longer-term technologies will appear, making the use of personal computers even more complicated.
- Open (free) software, for the time being the main alternative to the American giant software corporations, will continue to evolve, no longer primarily intended for a target population of professionals and experts and offering an interesting alternative to the American software monopolies
- Computers will require systematic installation of active semantic firewalls, considerably limiting direct attacks. In fact, the increasing mobility of computers, electronic diaries, telephones, etc. imposes the need for effective security at each point in the network.
- Screening of email messages will become a function of efficiency: the number of the daily emails will be significantly higher than postal service deliveries, while their usefulness or interest will be highly variable (from urgent messages to spam).
- Setting up a quarantine zone around or within the computer will become necessary considering the trend in the speed of data transfers between computers.
- Proof of identity (authentication) by certifying the authenticity of a heading, label, digital watermarks.
- Auditing of events, accountability and recording system history, starting with sensors and probes, traceability of the movements of various subjects and objects.
- Proof of communication (non-repudiation protocols), consent based on digital signatures of all kinds.
- Protection of the transport, processing, storage and archiving of documents, databases, transactions and operations.

- Management of copyrights and liabilities of owners, authors, distributors and subscribers: protection against hacking, modification, plagiarism and redistribution.
- Screening of access and authorizations in accordance with the security policies including adjustability to variables of time, space and context.
- Security management: administration of the security tools and mechanisms.

7.3.6 FP6: DESEREC (IST-2004-026600):

The DESEREC IST-2004-026600 (Dependable Security by Enhanced Reconfigurability) is an FP6 project that aims to improve the dependability of new and existing information systems by leveraging their capabilities of: Failure-proof, Self-healing, and short Recovery time [60].

To achieve these goals it takes a three-tiered approach:

- Prevent: keep every incident local
- React: sustain or quickly resume the critical services
- Plan: reallocate optimally the resources to recover the full range of services

DESEREC's research is focused on building service resilience against internal hardware or software failures and internal or external attacks or malicious actions. The project has currently only identified short to medium term challenges and still has to investigate long term FP7 orientated issues. However, the medium challenges highlight areas of early FP7 research in particular between the years 2007 and 2010.

Short-term Security & Dependability challenges:

- Modelling of Information systems appropriate for dependability management: containment, reconfiguration
- Early detection and reliable assessment of incidents (With a pattern-free approach)
- Dependability-oriented simulation

Medium-term Security & Dependability challenges:

- Automatic reconfiguration decision
- Computer-aided feedback on detection and reconfiguration rules
- Configuration management at I.S. level with fallback capability
- First quantitative approach of resilience assurance

Common themes:

DT-Dependability and Trust Initiative

SP-Policy Consensus Initiative (for reconfiguration of I.S.)

Common challenges:

DT: Rethinking availability

SP: System modelling

New proposed challenges:

DT: Monitoring the behaviour of Information systems

SP: Dependability-oriented modelling

7.3.7 FP6: ANTIPHISH (IST-027600)

AntiPhish (Anticipatory Learning for Reliable Phishing Prevention) is an FP6 project that will address researching adaptive filters that are not only able to identify variations of previous phishing messages, but are capable to anticipate new forms of phishing attacks. This technology would greatly improve all existing methods used in spam and phishing filters. AntiPhish aims at developing filters with unprecedented accuracy which are able to block more than 90% of phishing without blocking more than one legitimate email in a million [53].

The research will be driven by the hands-on expertise of our industrial participants, who have long experience with spam fighting on a global scale and will provide huge amounts of real world training data. The AntiPhish project not only aims at developing the filter methodology in a test laboratory setting, but has the explicit goal to implement this technology at internet service providers to be used to filter all email traffic online in real time, as well as content filtering at the edge of wireless networks.

7.3.8 FP6: S3MS (IST-027004)

The S3MS (Security of Software and Services for Mobile Systems) IST-027004 project is an FP6 project that aims at the development of a framework for trusted deployment and execution of communicating mobile applications in heterogeneous environments. S3MS would enable the opening of the software market of nomadic devices (from smart phones to PDA) to trusted third party applications beyond the sandbox model, without the burden of roaming trust infrastructure but without compromising security and privacy requirements [50].

The project aims to investigate:

- Security and Dependability by Contract
- design for inherent security & dependability
- exploitation of existing dependability and security capabilities
- Dealing with (but not relying entirely on) security infrastructures
- Security-by-contract,
- a mobile contract that an application carries with itself.
- A mobile-code policy that a platform specify
- What’s in a code’s contract?
- the relevant (security) features of the application
- the relevant (security) interactions with its host platform
- A proof –of compliance that code satisfies contract
- What’s in a platform’s policy?
- Platform contractual requirements on application
- Fine-grained resource control
- the mobile policy should be matched by the application’s contract and enforced by the platform

S3MS has highlight its main challenges as follows [51]:

Short Term:

- Associate a semantics to app signature

- Help mobile operators define their security policies
- Provide tools to check compliance to these policies
- Early result of the project

Medium Term:

- Introduce the notion of contract
- Personalize the operator/developer relationship
- Allows developer to work independently of operators

Long Term:

- Generalize contracts and policies
- Introduce end-user policies, policy combination, ...
- Fine-grained resource control
- Concept ready at the end of the project
- Language-based Security
- Major issue in NSF Programmes
- Security Engineering
- Integrated approach beyond pure technological solutions
- Steps in Secure Application Development and Deployment
- Security Requirement capture
- Secure (code) Development Tool Support
- Security Technology Solutions
- (Automatic) Configuration and Management

7.3.9 FP6: FASTMATCH (IST-027095)

FASTMATCH is an FP6 project that directly addresses the need to create a layered and agent-oriented architecture to enable delivery of multiple pattern-based and behaviour-based scanning and filtering functions at much higher speeds than realised by the state-of-the art. The major technical objectives are to provide a framework for the concurrent operation of reactive and proactive security algorithms, to deliver algorithmic enhancements for pattern recognition and behaviour-based detection schemes, as well as enhanced and highly correlated rule sets for more efficient alarm management and root-cause analysis. It is important to point out that the tools developed by FastMatch will be robust in the sense that they will seek to constantly adapt and react to changing security threats in the longer term [52]. Detailed objects of the project are described below [51, 52]:

- Threat source identification and localisation (switch interface, geographic location, source Service Provider, etc.), thus supporting network-wide threat resolution and communication with a higher management application or Authority to take actions on the network itself, such as blocking the threatening device or alerting the source Service Provider.
- A new generation of security management architecture based on a Multi-Agent System to model and implement an intelligent intrusion detection system. The goals are to detect known and unknown attacks, as well as to minimise the number of false alarms

arising from the single-model, and thus uncorrelated approach to deployment of either signature-based or anomaly-based detection algorithms alone.

- The achievement of higher levels of correlation (and thus less false or indeterminist alarms) by combining both signature and behaviour/anomaly–based models within a framework of multiple dissimilar security protection functions (pattern scanning and intrusion detection for instance) as well as combining such results with session context, topology and location-specific information.
- To run multiple function types at higher speeds than currently realisable within an FPGA-based architecture, so as to leverage its programmability attributes, and determine how best to supply correlation enablers to feed post-threat identification processing tasks. As a feedback loop, the work will optimise the real-time processing achieved, as well as the individual and correlation-oriented post-processing tasks.
- To investigate parallel processing algorithms to determine whether sufficient efficiencies can be achieved to scale an FPGA-type architecture towards 40 gb/s or above. The speed objective is closely tied to permitting security functions to be deployed at the core of the network as a key component of a multi-layer security architecture allied to gateway, desktop and other perimeter functions.
- To develop a massively parallel Genetic Programming (GP) hardware model in order to evolve more efficient rules using the initial rules compiled on the basis of background knowledge from known attacks and also to explore alternative techniques such as the Genetic Algorithm (host, network monitoring, rules evolution), Niching technique to produce multiple rules (sequential niching technique, deterministic crowding), and, Immuno-Fuzzy approach to anomaly detection (use of fuzzy rules instead of crisp rules to cover the non-self space i.e. fuzzy detectors), within a methodological framework for evolutionary programming approaches for detecting intrusions.
- Specifically, in this project we shall apply the bio-informatics Smith-Waterman algorithm for masquerading malware detection (an intruder assuming the identity of a legitimate user) as well as other bioinformatics tools such as Similarity Matrices, Phylogenic Trees and Multiple Alignment for Protocol Analysis. The results can be extended to computer forensics (looking for hidden strings on hard drives), analysis of the habits of web visitors etc.

7.3.10 FP6: SERENITY (IST-027587)

SERENITY (System Engineering for Security & Dependability) is an FP6 project that will enhance security and dependability for Ambient Intelligent (AmI) ecosystems by capturing security expertise and making it available for automated processing. SERENITY will provide a framework supporting the automated integration, configuration, monitoring and adaptation of security and dependability mechanisms for such ecosystems. [51, 54].

Objectives include:

- To make validated security solutions available to AmI ecosystems and promote their assurance and evolution
- To support the definition of security requirements which arise in business, private and legal activities in order to enable a requirements-driven selection of appropriate security mechanisms within integration schemes at run-time.
- To provide mechanisms for monitoring security at run-time and dynamically react to threats or breaches of security and context changes

- To integrate SERENITY security solutions, requirements definition, solution selection, and monitoring and reaction mechanisms in a common framework
- To capture security expertise in such a way that it can be supported by automated means.
- Materialization of the concepts of “Security and Dependability Pattern” and “Integration Schemes”.

Main challenges include:

Short term Challenges [51]:

- Enhanced notion of S&D Patterns and Integration Schemes (short-term)
- Computer aided run-time monitoring of the implemented security solution (short-term)
- Medium-term - for 1st phase of FP7 2007 – 2010

Medium Term Challenges [54]:

- Security & Dependability only at application level
- Security and dependability considered as the last issue
- Security and dependability faced, mainly, from a technological point of view
- Security and dependability "applied to relatively stable, well-defined, consistent configurations, contexts and participants to security arrangements"

Long Term Challenges [54]:

- "conformable security"
- Social, political, ethical, technological aspects to be considered
- Heterogeneity, mobility, size, complexity, ...
- Distribution of knowledge
- data protection wrt. the operative context (privacy, anonymity, etc.)
- Communication infrastructures and hardware devices not under the control of the security engineers

7.3.11 FP6: IRRIIS (IST-027568)

IRRIIS is an FP6 project that addresses the area of Complex Information Infrastructure Protection (CIIP). It will enhance substantially the dependability of Large Complex Critical Infrastructures (LCCIs) in the sectors energy supply and telecommunication by introducing appropriate Middleware Improved Technology (MIT) components and developing a synthetic simulation environment for experiments and exercises (SYNTEX) [51, 55].

Objectives include:

- determine a sound set of public and private sector requirements based upon scenario and related data analysis
- design, develop, integrate and test MIT components suitable for preventing and limiting cascading effects and supporting automated recovery and service continuity in critical situations
- develop, integrate and validate novel and advanced modelling and simulation tools integrated into the SYNTEX environment for experiments and exercises

- validate the functions of the MIT components using the SYNTEX environment and the results of the scenario and data analysis
- disseminate novel and innovative concepts, results, and products to other ICT-based critical sectors

Within duration of project:

- CIIP research not well developed until now
- identification and modelling of LCCI interdependencies
- integration of MIT components and existing tools into SYNTEX environment

After project completion further use of the generic SYNTEX environment:

- in other LCCI sectors than energy supply and telecommunication
- digital double of the communications network infrastructure of two typical European countries
- digital double of a midsize city with citizens (with real-life behaviour) and all infrastructures

7.3.12 FP6: HIDENETS (IST-026979)

The HIDENETS FP6 projects will develop and analyze end-to-end resilience solutions for distributed applications and mobility-aware services in ubiquitous communication scenarios. The project intended to develop applications with critical dependability requirements in the context of selected use-cases of ad-hoc car-to-car communication with infrastructure service support. The HIDENETS solutions are expected to contribute to a user perception of trustworthiness of future wireless services, as this perception is strongly impacted by availability and resilience aspects. Such perception is critical for the technical and business success of these services [51, 57].

Objectives include:

- Develop and analyze end-to-end resilience solutions for scalable distributed applications and mobility aware services
- In ubiquitous communication scenarios. Example use-case: car2car communication with server-based infrastructure assuming highly dynamic, unreliable communication infrastructures
- Dynamically changing communication characteristics in ad-hoc domain and in connection to infra-structure services
- Off-the-shelf, standard systems and components in both domains
- Services with high dependability and scalability requirements

Short Term Challenges:

- Selected use-case of ad-hoc car-to-car communication with connectivity to infra-structure services work with standards groups (SAForum, C2CC)

Medium Term Challenges:

- Applicable in other, related scenarios, including Personal Area Networks and cellular networks with ad-hoc coverage extension interface to related standards and open source activities (W3C, Java, Eclipse)

Longer Term Challenges:

- Common themes: security and reliability are two sides of a coin
- Common challenges: dependability requires integrated view on security and reliability/availability cost aspects
- New themes/challenges that need to be included in STF: standard interfaces, methods and tools during complete product life cycle, interfacing to standardization bodies, integration with and use of COTS environments

7.3.13 FP6: CRUTIAL (IST-027513)

CRUTIAL (Critical UTility InfrastructurAL Resilience) is an FP6 project that will addresses new networked ICT systems for the management of the electric power grid, in which artefacts controlling the physical process of electricity transportation need to be connected with information infrastructures, through corporate networks (intranets), which are in turn connected to the Internet. It will investigate modelling interdependent infrastructures taking into account the multiple dimensions of interdependencies, and try to cast them into new architectural patterns, resilient to both accidental failures and malicious attacks [56, 51].

Objectives include:

- Provide modelling approaches for understanding and mastering the various interdependencies among power, control, communication and information infrastructures
- Investigate distributed architectures enabling dependable control and management of the power grid

Main challenges:

- Modelling interdependent infrastructures taking into account the multiple dimensions of interdependencies, and attempting at casting them into new architectural patterns, resilient to both accidental failures and malicious attacks
- Analyse the impact of information and computer failures on the electric power outages
- New threats and vulnerabilities emerge from tight coupling of power, control, communication and information infrastructures and from evolving control systems
- Resilient power control in spite of threats to their information infrastructures

Common challenges

- Resilience of heterogeneous ICT systems
- Resilience of open communication infrastructures
- Multiple threats to critical ICT applications
- Comprehensive framework for modelling & evaluating resilience
- Dependability and security case for interconnected utility infrastructures

7.3.14 FP6: CI^{2}RCO (IST-2004-15818)

CI^{2}RCO (Critical Information Infrastructure Research Co-ordination) is a FP6 Coordination Action Project that aims to carry out a gap analysis of critical infrastructure that compares needs to existing research programmes and to determine R&D priorities based on relative importance of different needs, likelihood of R&D success and the timeframe in which R&D occurs [59].

In summary the projects main objectives are:

- create and co-ordinate a European Taskforce to encourage a coordinate Europe-wide approach for research and development on Critical Information Infrastructure Protection (CIIP), and establish a European Research Area (ERA) on CIIP as part of the larger IST Strategic Objective to integrate and strengthen the ERA on Dependability and Security
- the CI^{2}RCO consortium further on aims to support CIIP awareness and actions in the EU-25 and Associate Candidate Countries (Bulgaria, Romania, Turkey) in order to:
  - provide a forum and a platform to bring together the different key players to exchange experiences, share interests and define areas for joint activities,
  - identify key dependability and security CIIP challenges,
  - foster truly multidisciplinary and innovative approaches to research that would build on the contributions provided by diverse scientific communities,
  - encourage and support the national and international co-operation on key global CIIP research issues,
  - develop recommendations and a roadmap for current and future CIIP research activities,
  - support policy-makers in charge of financing or managing R&D programmes.

7.3.15 FP6: ReSIST (IST-026764)

ReSIST (Resilience for Survivability in IST) is an FP6 network of excellence (NOE) project which started in January 2006 aims at researching the requirement for resilience, self-healing, dynamic content and volatile environments [65].

The objectives of the NOE are:

- Forming the right research team so that the fundamental topics concerning scalable resilient ubiquitous systems are addressed by a critical mass of co-operative, multi-disciplinary research.
- Identification, in an international context, of the key research directions (both technical and socio-technical) induced on the supporting ubiquitous systems by the requirement for trust and confidence in AmI.
- Production of significant research results (concepts, models, policies, algorithms, mechanisms) that pave the way for scalable resilient ubiquitous systems.
- Promotion and propagation of a resilience culture in university curricula and in engineering best practices.

7.3.16 FP6: POSITIF (IST-2002-002314)

POSITIF (Policy-based Security Tools and Framework) is an FP6 project that aims to create a policy-based unified security framework that will enable different kinds of security tools to be integrated. A multi-level policy language will be used to describe the desired security policy (SPL) while a system language will be used to describe the target system (SDL). A checker will evaluate if the desired policy can be implemented on the target system and will measure the achieved security level. Configurations for the security elements will then be automatically generated and deployed through the network. A monitor will use the security policy for proactive intrusion detection in addition to standard reactive intrusion detection. The framework will be usable by any producer of a specific security block or tool due to the use of open standard based languages, interfaces and protocols for policy and system description, configuration instructions and deployment, threat monitoring. This framework will be complemented by a suite of security tools including high speed firewall, VPN and IDS that target the current challenges and a lightweight security module to protect them against network attacks, make them part of the security system and allow secure downloading of new configurations [67].

Challenges the project aims to address:

- Multiple access ways: wired/wireless; PC / PDA / Mobile Phone
- New applications with new challenges: P2P, large scale multimedia applications
- Multiple vendors and hardware/software-platforms due to the growing of nodes and needs within the network
- Decreasing the amount of intrusions / spam within networks
- Better security tools and moreover a better coordination among these tools
- A reliable / guaranteed answer to the question: "will my network fulfill the desired security needs?"
- An automated support for handling alerts within the network. Or even better: a proactive system that continuously checks the network and provides a self learning mechanism through the handled alerts, attacks and other critical events.

The POSITIF project were the main drivers for the established Security Policy Initiative in the Security and Dependability Task Force.

7.3.17 FP6: TRUSTCOM (IST-2002-002314)

The goal of the TrustCoM integrated project is to provide a trust and contract management framework enabling the definition and secure enactment of collaborative business processes within Virtual Organisations that are formed on-demand, self-managing and evolve dynamically, sharing computation, data, information and knowledge across enterprise boundaries, in order to:

- tackle collaborative projects that their participants could not undertake individually or
- to collectively offer services to customers that could not be provided by the individual enterprises.

Such VOs will be based on new forms of collaboration in which participants (enterprises or individuals) can specify and negotiate their own conditions of involvement by means of electronic contracts whose operation is supported and enforced by the computing infrastructure. Such collaborations can be established only in a secure environment where the controls and procedures are automated based on clear specifications of trust, risk and policy.

To achieve these goals, TrustCoM will conduct multidisciplinary research into complex, adaptive and self-organising systems in order to deliver a novel trust and contract management reference framework that will enable collaborative work within on-demand created and self-managed dynamic collaborative networks of businesses and governments built on top of the emerging convergence of Web Services and Grid technologies.

7.3.18 FP6: ESFORS (FP6-027599)

ESFORS (European Security Forum for Web Services and Systems) is an FP6 Coordination Action project that aims at bringing together the European stakeholders for security and dependability Information and Communication Technologies (ICTs) to address the security and dependability requirements of emerging software service platforms. The project is currently in its infancy. The project is positioned to support the emergence of a software and services platform architecture ensuring the incorporation of security and dependability best practice. The expected key outcomes from the project are [51, 62]:

- The establishment of a pan European Industry and Academic forum addressing security and dependability issues for software, services and systems
- The development of a Strategic Security Research agenda in support of FP 7 research initiatives on software and services
- The specification of an Industry framework, agreed by European stakeholders, for security, dependability and resilience of systems, services and infrastructures.

The objectives of ESFORS (Co-ordination Action project) include the definition the security research challenges in the software and services domain, contribution to the FP7 research agenda, contribute to the NESSI SRA, promoting networking of European stakeholders on security and dependability strategy, guiding direction of Security and Dependability research in the ESRA on Software and Services and to strengthen interplay between research and policy communities within software & services arena.

The project intends to build industry awareness of the need for security in software-based services and systems, foster joint efforts among research, industry and policy makers and to involve organizations rather than individuals only in the software community.

7.3.19 FP6: GRID (FP6-026923)

The background of the GRID FP6 project pertains to the increased vulnerability of the electrical infrastructure, which appears to be growing due to enlarged demand, hectic transactions, growing number of stakeholders, complexity of controls, as made patent by the major recent blackouts over Europe and North America. Although these events don't seem to have been influenced by malicious acts, existing vulnerabilities could be exploited by malicious threats in the future. The GRID project will establish a consensus at the European level on the key issues involved by power systems vulnerabilities. The main objectives of GRID are [58, 51]:

- Analysis of the different security issues, the current knowledge and bottlenecks, the on-going or planned initiatives and researches, directly or indirectly linked to the topic;
- Identification of research priorities – road mapping;
- Identification of recommendations to be issued for security policies;
- Raising awareness on the security concerns at the policy, industrial and academic level.

Two of the main topics proposed to date are:

- Methods to assess reliability, security and risks affecting the power grid, especially concerning vulnerabilities arising from the increased control complexity and to the openness of the supporting information and communication technologies;
- Management, control and protection schemes and the relevant architectures and devices

On these areas, GRID will assess the needs of the power sector and achieve consensus among stakeholders and R&D institutions, so as to establish a roadmap for collaborative R&D on innovative and/or advanced technologies pertaining the two target areas.

7.4 Mobile, Wireless & Smart Card Research

There were two roadmap projects within this area of research including PAMPAS: Pioneering Advanced Mobile Privacy and Security and RESET: Roadmap for European research on Smartcard related Technologies.

7.4.1 FP5 Roadmap: PAMPAS (IST-2001-37763):

Pioneering Advanced Mobile Privacy and Security (PAMPAS) was a FP5 roadmap project that addressed security, privacy and identity management as key factors of the user acceptance and commercial success or failure of new mobile systems and services beyond the third generation [39]. The project has released a roadmap that describes research challenges for security and privacy in future mobile communication systems.

The research challenges deemed most critical were described [40]:

Trusted mobile devices - secure and user friendly: Trusted paths from the mobile device to the user needs to be foreseen. A good balance should be found between allowing potentially dangerous tools (such as cookies and mobile code) and enforcing the appropriate usage of them (i.e., in security applications). Also highlighted was the need for substantial research and development efforts concerning trusted execution environments (operating system and hardware platform) for mobile devices.

There needs to be more research into and development of mobile devices that provide just enough user-friendly functionality and still remain authentic and trustworthy.

Full exploitation of the SIM card:

Extend SIM card beyond just authentication. The SIM can provide a number of different security functions therefore it has to be researched.

Secure reconfiguration of mobile devices:

Secure reconfiguration issues concerning authorisation, data origin and integrity, privacy, and conformance with regulatory requirements have to be investigated.

DRM security architecture and protocols:

A good DRM system should possess tamper-resistant memory, tamper-resistant execution environments, tamper-resistant network interfaces, secure clocks, device specific keys and certificates. There is a need to develop DRM systems to a better maturity.

Protection of the core network against attacks:

Mechanisms need to be researched that reduce the risk of attacks against the core network in particular protection against Denial-of-Service attacks.

Heterogeneous network access control security:

Authentication and key agreement is the central component of secure access procedures. Currently, there are no protocols available that are light-weight, can be carried over arbitrary access networks and are flexible enough to be re-used in many different contexts in future mobile systems. The development of new authentication protocols may be required here.

Seamless security handover at network level:

Re-authentication often causes prohibitive delays, so efficient security context transfer schemes are needed. Security solutions still need to be developed for seamless handover between different network types.

Security architectures for service networks:

The internal and inter-domain security architecture within service networks is still in its infancy and needs to be researched in detail.

Protection of the service network against attacks:

Research in service network protection is of utmost importance. Protection using intrusion detection, cryptographic measures and so forth.

Mobile application security framework:

Given the growing heterogeneity of the user's communication environment, there is a need to develop and validate a coherent framework for security and trust for mobile applications.

User centric mechanisms allowing controlled release of personal information:

User-centric mechanisms are required to allow controlled release of personal, preference-related and location-based information, and to deliver assurances to owners about how personal information will be used by third parties.

Single sign-on based on mobile authentication:

Mobile operators could play an important role in single sign-on solutions. Investigations should include not only technical aspects but also end user experience.

Authorisation privacy:

Authorisation plays a particular role on privacy, since personal information is distributed to enable access control. In particular, the client-server model, on which most Internet applications are developed, can be considered as privacy-intrusive: generally, the server grants or denies access to a client according to the identity claimed by the client. The management of multiple identities raises problems of ease-of-use, as well as unlinkability. Another related approach is to use cryptographic functions to prove certain attributes of a certificate without disclosing other attributes. Pampas has highlighted the need to research solutions and experiments on large-scale operations should also be supported.

Authentication via security tokens using mobile devices:

Mobile devices can be used as a security token. Research is needed in the area of challenge-response techniques via wireless devices. These solutions also need to be standardised so that it should be possible to use any conformant mobile device as a security token in authentication protocols.

Location based services versus location privacy:

The user may be provided with certain services having properties based on his/her location context. However, the user may wish to keep his location private. Hence, there is a need for location-based services, which preserve location privacy.

Privacy preserving mobile applications with tuneable anonymity:

There are technologies that provide (data) anonymity and are aimed at protecting the user's privacy to some determined extent. In some cases this is achieved at the cost of loss of functionality. Further research and evaluation of application-specific privacy-preserving solutions is needed.

Lightweight stream ciphers:

Research is needed to develop lightweight stream ciphers with a well-understood level of security for application in constrained environments. Pampas notes that current efforts such as the NESSIE project have not resulted in such primitives.

Truly practical cryptographic mechanisms in constrained environments:

Practical the cryptographic mechanisms associated with payment, digital rights management, privacy and anonymity protection is a challenge to cryptography from mobile applications point of view. These mechanisms include special signature schemes, electronic cash schemes, and key exchange and authentication protocols.

Delegation of cryptographic operations:

Pampas has highlighted the need for further research to develop mechanisms that support delegation of cryptographic operations from constrained mobile devices to more powerful but less trusted devices.

Lightweight key management infrastructures:

There is a need to develop and standardise lightweight key management infrastructures supporting the deployment of public key technology in mobile networks, and to ensure the interoperability of infrastructures from different mobile standards.

Conference and group keying:

Multi-party mobile communications require the existence of efficient cryptographic protocols for dynamic conferencing and group keying.

7.4.2 FP5 Roadmap RESET (IST-2001-39046)

RESET (Roadmap for European research on Smartcard related Technologies) is an FP5 roadmap that aimed at investigating the research requirements corresponding to current and expected future technology gaps, identified by the industry and resulting from market and product trends foreseen by smart card industrial players. RESET details current and future challenges on secure devices and platforms [45].

The project resulted in defining 6 main technology areas, each of them covered by one expert working group in the following areas:

- Communication & Networking
- Systems & Software
- Smart card accepting devices, interfaces & biometry
- Card embedded peripherals, subsystems & micro-systems
- High-end cryptography, tamper-proof and security technologies
- Micro-electronics.

1. Communication & Networking:

The scientific and technical challenges highlighted by RESET are:

Performance improvement:

- The smart card needs to enhance its communication capabilities, according to the state of the art in the world to which it is connected. It is necessary to improve the interface in both the wired and wireless modes.

Connectivity enhancement:

From a communication and networking standpoint, the evolution towards open platform will be achieved when the smart card is the position of being smoothly integrated into the interconnected IT world. The following targets should be considered:

- TCP/IPv6
- Security of the link
- Wireless protocols

Support new communication model:

True multi-applications smart cards require that different applications could simultaneously have access to resources available (communication stack, NVM memory, etc.). This will undoubtedly impact the underlying Operating System. In this context, following topics seem to be relevant:

- Multi-tasking OS
- faster NVM access
- enhanced RAM capacity

2. Systems & Software:

Operating Systems & High Level Languages:

Flexible, multi-application smart card environments should be supported by appropriate operating systems with standard operating system (OS) features, such as multi-threading and high-level memory management, and new OS features required by smart cards, such as resource control management (deadlock prevention/detection, optimised resource usage), or enhanced transactions (in particular with respect to multi-threading). The future should target micro-kernels that support different smart card platforms, and opensource OS with expected benefits of portability, flexibility and interoperability. They could help smart cards to evolve towards full-fledged, secure autonomous computers and could make the smart card a full partner on the network, for example by allowing to connect to a smart cards like to an ordinary web server, from web browsers via IP address or network name, by using XML protocol to enable XML based card applications, and by supporting a variety of application frameworks (Java,.NET, HTML, XML) in a single card.

Development Tools:

Programming languages for smart card applications should be made more intuitive like general-purpose programming languages (Java). Precise validation strategies are required to determine where provability and testability could collaborate or supersede each other; in particular, it would be highly desirable to device methods to decide when a test is pertinent enough to substitute for a proof.

- Design modelling languages that are sound and expressive, yet remain usable in practice.
- Develop adequate interfaces between these modelling languages and existing theorem provers and model checkers.
- A range of dedicated development tools should emerge, that are cost-effective and accessible to non-experts.

Systems Integration & Card Application Management:

The use of formal modelling and formal verification needs to be supported.

There is a strong need to develop environments that support, in a cost-effective manner, all aspects of certification: risk analysis, edition of security targets, system design and development via checked refinements, testing, formal modelling and verification. System Integration should be improved through integrated tools that permit the development of applications in a global framework.

- These tools should fit in different usage scenarios: 3G Mobile Networks, TCP/IP based networks, etc.
- New design models and design methodologies should be sought.
- Extensible and scalable on-card and off-card framework, dynamic management of card framework services, etc.
- To achieve such goals, it is mandatory that adequate OS are used.

3: Smart card accepting devices, interfaces & biometry:

There are a large number of challenges identified here that need to be addressed to link the synergies of the actual devices, their interfaces and biometric possibilities:

- Terminals will need to support new formats in addition already established formats.
- Cards with other form factors should become possible, such as thinner ID1 cards (<0.4 mm). New form factors will impact the read/write interface.
- Use of increased functionality and the ensuing interfacing (and standardisation) will require further work.
- In the context of standard architectures, such as STIP, FinRead and Global Platform, the implementation of common test suites and of security certification procedures is a major requirement of the smart card industry as a whole.
- High speed protocols: The card reader needs to support new protocols that will allow for higher data rates
- It will be necessary to add new physical interfaces to ease integration in existing infrastructure, e.g. a PC interface via USB, and a PDA interface via Blue-tooth.
- The 5 Volt power supply is the de facto standard for POS terminals, whereas mobile phones operate at 3 Volt. These voltages will be reduced to lessen the energy demands of (mainly battery powered) devices. This requires redesign of terminals and revision of standards.
- There are many ways in which biometrics can be deployed to capture some distinguishing element of the biological makeup of a person. Some of these (face recognition, hand geometry) are perhaps less easy to include in smart card based systems. Others would seem ideally suited to improve the security of smart cards. These include finger prints, voice recognitions. The challenge is in the (on-card or off-card) integration, deployment, management and user acceptance.
- Instilling trust in the user of the card.
- Make smart cards more in tune with every day pervasive objects such as watches, key rings and so forth.

4. Card embedded peripherals, subsystems & micro-systems:

There is a requirement to address the following research areas:

Standard hardware architecture:

- Interface between main chip and bus: managed by a separate interface chip (the interface should not be included in the main chip).
- Interface between bus and display: managed by an "already mounted on the display" chip.
- Interface between the separate interface chip and the knobs: direct connection, no need to be driven by the bus.
- Interface between the separate interface chip and the battery: direct connection, no need to be driven by the bus.
- Display: mono or bi-stable, segmented or pixel.
- ISO 14443 (13.56MHz) optional RF interface included in the separate interface chip: the antenna is connected to this chip and not to the main chip.
- Extended range of peripherals (biometric sensors, MEMs), all supplied with their interfaces "already mounted on".
- Increased on card memory

Power Supplies:

- Primary and secondary batteries
- Voltage: from 3 / 4 Volts to 1,8 Volts
- Capacity: in the range of 25 mAh, depending on application profile.

Packaging technologies:

- Thinner (below 100µm) wafers handling and improved chip packaging

Interconnections technologies:

- Flip chip technology for contactless and tags
- Lead-free components (as in *wires*, not *Pb*)
- Cost effectiveness through reduced thicknesses, and connection density

5. High-end cryptography, tamper-proof and security technologies:

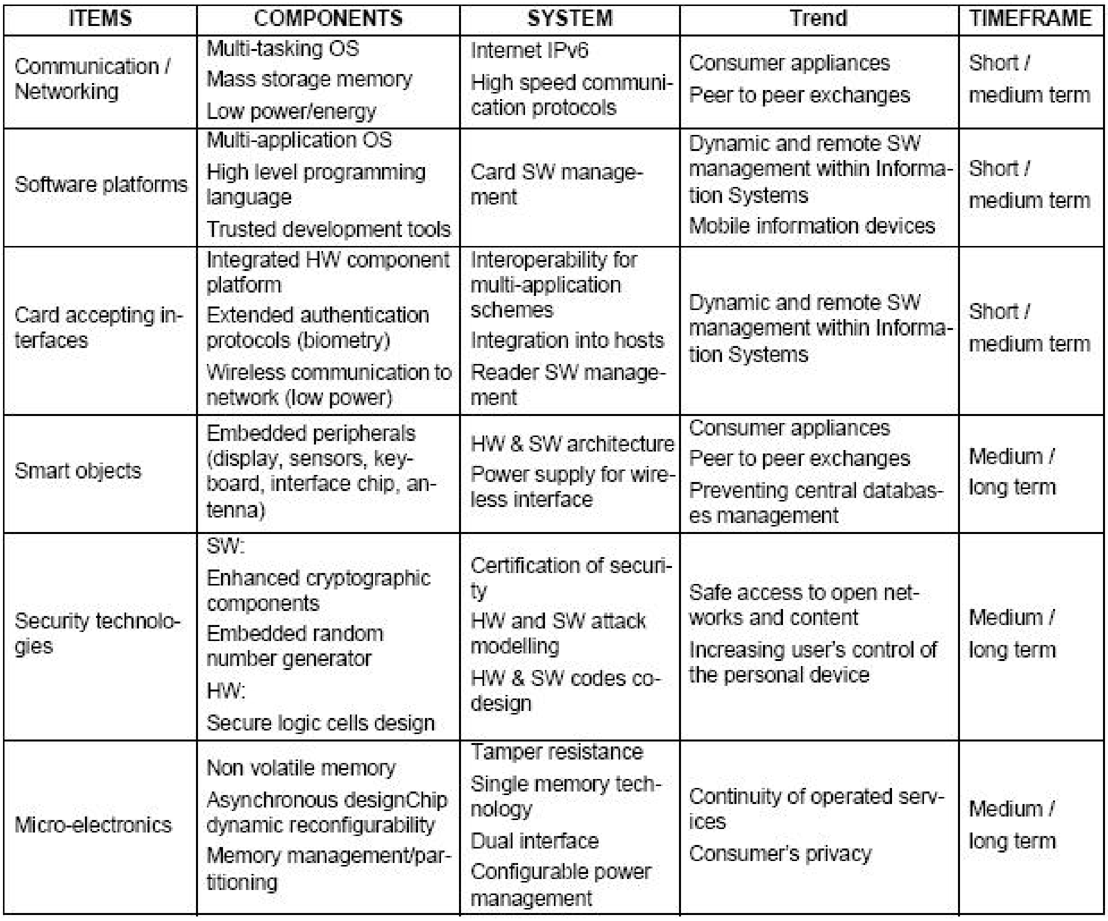
New avenues for increasing the speed of the cryptographic procedures even with longer keys and both secure and practicable key management systems are required. Research will need to address the following:

- New crypto protocols
- Increase of key sizes for more secure authentication
- New signature protocols
- Elliptic curve capabilities inbuilt on the card
- Tamper-proofing
- Formal modelling
- On-card random number tests
- New attack countermeasures
- Secure software

6. Micro-electronics:

- Die size optimization (for cost effectiveness)
- Packaging environment
- Security requirements
- Performance optimization:
- Platform architecture
- Power consumption continuous reduction
- Easy third party IP integration and re-use
- IP protection through design
- Rapid and cost effective development environment
- Compliance with Semiconductor Industry technology road map (ITRS reference)
- Integration of reliable, flexible and fast high-density Non Volatile Memory technologies, with high density RAM.
- Dynamically re-configurable devices, on a longer term
- Endless challenge for meeting the security requirements versus the technology limits created by the ITRS road map, as well as cost and testability constraints.

In summary the following table shows the projects synopsis:



ITEMS	COMPONENTS	SYSTEM	Trend	TIMEFRAME
Communication / Networking	Multi-tasking OS Mass storage memory Low power/energy	Internet IPv6 High speed communication protocols	Consumer appliances Peer to peer exchanges	Short / medium term
Software platforms	Multi-application OS High level programming language Trusted development tools	Card SW management	Dynamic and remote SW management within Information Systems Mobile information devices	Short / medium term
Card accepting interfaces	Integrated HW component platform Extended authentication protocols (biometry) Wireless communication to network (low power)	Interoperability for multi-application schemes Integration into hosts Reader SW management	Dynamic and remote SW management within Information Systems	Short / medium term
Smart objects	Embedded peripherals (display, sensors, keyboard, interface chip, antenna)	HW & SW architecture Power supply for wireless interface	Consumer appliances Peer to peer exchanges Preventing central databases management	Medium / long term
Security technologies	SW: Enhanced cryptographic components Embedded random number generator HW: Secure logic cells design	Certification of security HW and SW attack modelling HW & SW codes co-design	Safe access to open networks and content Increasing user's control of the personal device	Medium / long term
Micro-electronics	Non volatile memory Asynchronous designChip dynamic reconfigurability Memory management/partitioning	Tamper resistance Single memory technology Dual interface Configurable power management	Continuity of operated services Consumer's privacy	Medium / long term

The following FP6 projects were supported based upon a number of the recommendations of these roadmap projects or are carrying out work relevant to the projects.

7.4.3 FP6 MOSQUITO (IST 004636):

The MOSQUITO (IST-2002-506883) project, is a an FP6 STREP project that aims at developing a framework for implementing secure and adaptive business applications for mobile workers. Such applications would rely to great extent on various types of context information in order to adapt both its logics and its security measures [46].

The MOSQUITO project makes a distinction between *secure context-awareness*, which focuses on ensuring availability, authentication, integrity, confidentiality of context-aware information, and *context-aware security*, which focuses on using context information in order to optimise and adapt security measures employed within distributed business applications [47].

The context information utilised for the context-aware computing can vary substantially, e.g. it can describe computing and the physical environment, time, and user's state. It can also differ in regard to its persistence (e.g. static, dynamic), origin (e.g. internal, external), and quality (e.g. timeliness, coverage, resolution, and accuracy).

One of the challenges in distributed systems is the aggregation of context data from different providers. In particular, the challenges of malicious parties trying to provide false date in order to influence the final result of aggregation. Appropriate robust statistical methods and trust evaluation algorithms need to be implemented to ensure the trustworthiness of context information.

Context information can be used as input to many security-related processes, such as access control, authorisation and trust management. Context information can be used for (re)-

configuration of security mechanisms, too. But looking at security in this space it is a trade off between optimisation and introducing new vulnerabilities.

Mosquito has highlighted three main security challenges related to context-aware computing [47]:

- Confidentially of context info
- Integrity of context info.
- Availability of the context info.

Researching these key challenges help to ensure the security of the new context aware systems against context spoofing, DoS attacks and so forth. Secure context-awareness is fundamental for ambient intelligence. Also, privacy protection is an important, although often neglected, part of context aware applications.

7.4.4 FP6: DAIDALOS (phase 1: IST-2002-506997, phase 2: IST-2005-026943)

DAIDALOS (Designing Advanced network Interfaces for the Delivery and Administration of Location independent, Optimised personal Services) is an FP6 projects that aims at providing mobility within business, education, and leisure activities of European citizens. The DAIDALOS approach is seamlessly integrating heterogeneous network technologies that allow network operators and service providers to offer new and profitable services, giving users access to a wide range of personalised voice, data, and multimedia services. DAIDALOS has identified a number of challenges categorised under Wireless & Mobile and Identity & Privacy Management [61].

Wireless & Mobile:

- Secure neighbour discovery: MIPv6 and AAA integration, key management, inter-domain challenges.
- Security within sensor networks.
- Regulatory aspects: Lawful interception, fraud detection and privacy enforcement.

Identity & Privacy Management:

- Interoperable and compatibility across standards.
- Stronger laws and regulations in particular enforcement and forensics.
- Societal changes particularly towards privacy behaviour.
- New virtual identity and privacy (VID) challenges focused on mobile applications. For example linkages between wireless and biometrics.

7.4.5 UbiSec&Sens (IST-2004-26820)

UbiSec&Sens (Ubiquitous Sensing and Security in the European Homeland) is an FP6 Specific Target Research Project (STReP) that started in 2006. Wireless Sensor Networks (WSN) requires research and development of an architecture for medium and large scale wireless sensor networks integrating comprehensive security capabilities right form the concept stage. This would support the rapid development of sensor networks and would open up the application domain for commercial activities.

The UbiSec&Sens research intends provide a comprehensive architecture for medium and large scale wireless sensor networks with the full level of security that will make them trusted and secure for all applications. In addition UbiSec&Sens will provide a complete tool box of security aware components which, together with the UbiSec&Sens radically new design cycle for secure sensor networks, will enable the rapid development of trusted sensor network applications [64].

To date, UbiSec&Sens has highlighted the following challenges [51]:

- To provide a security and reliability architecture for medium and large-scale WSNs acting in volatile environments.
- apply a radically new design cycle for secure sensor networks.
- To provide a complete toolbox of security and reliability aware components for sensor network application development.
- To focus on the intersection of security, routing and in-network processing.
- Solutions will be prototyped and validated in the representative WSN.
- Application scenarios of agriculture, road services and homeland security
- Flexible routing and in-network processing.
- Concealed data aggregation.
- Data aggregation with discrepancy query and multiple monitoring sensors.
- Encrypted distributed data storage.
- Enhanced key pre-distribution.
- Provably secure routing.
- Resilient data aggregation.
- Pairwise/groupwise authentication or re-recognition.

7.5 Biometric Research:

This section highlights the main projects of FP5 and FP6 and their recommendations for the way forward in FP7 in terms of biometric research. Within this section, one can get an overview of each of the project objectives and linkages to each other as research progressed in this subject area.

7.5.1 FP5: BioVision (IST-2001-38236):

BioVision (IST-2001-38236) was an FP5 roadmap project to lead the way forward for FP6 projects in the area of biometric research. The principle aim of the project was to address three key avenues: the first was to deliver a roadmap of future biometric research direction, which highlighted 38 prioritised areas of research. The second avenue addressed supporting studies that looked at the end-user perceptions, security, the legal and regulatory environment, medical perspectives, technology and applications and standards.. Thirdly, the project set up a biometric forum to assist in partnership collaborations in solving biometric challenges of the future [41].

The BioVision roadmap project outlines a number of challenges that where assigned a "key priority area" or an "important area". Below is a list of *Key Priority* challenges categorised under 6 headings [1]:

Systems & Design:

- RC/Sec1 - Methods are required to evaluate and compare the security of biometric systems.

- RC/Sec2 - Methods for the design and secure implementation of appropriately secondary systems that cope with both false match and false non-match errors.
- RC/Sec3 - Development of design methodologies that support the secure integration of biometric data in applications such as the Criminal Justice Sector, while limiting the opportunity for misuse. These could make use of binding of the user's identity, the application, template and user's expression of consent as well as validation by external Trusted Third Parties.
- RC/Sec4 - Biometric data for different applications (or held centrally and on-card) may require to be of different types (or held in incompatible formats) in order that centrally held information cannot be misused.
- RC/Sec5 - Provision of "live and well" features in biometric systems is a high priority, especially when these are unattended or only intermittently attended by security personnel. Testing of the liveness of the biometric signal needs to be commensurate with other security aspects of the system

Deployments:

- RC/Dep - High profile failures of bio solutions could impact its adoption, so it needs to be minimised.

Trial, Testing & Legal:

- RC/TTL4 - Database storage systems must be secure and trusted before becoming large scale public systems.

Products & Solutions:

- RC/PS1 - Transparent systems with excellent adaptive user interfaces delivering instantaneous authentication for end users.
- RC/PS2 - Systems that are easy to install securely, with useful and appropriate feedback if they fail.

Components:

- RC/C4 - Research into the ultimate limits of performance with various methods of implementing specific biometric techniques.
- RC/Csupp - Smart sensor development to improve performance, scalability, functionality, etc

Standards:

- RC/S1 - Interface standards are needed for all aspects of the operation of biometric systems.
- RC/S3 - Standards should be appropriate for specific application areas (including the legal and societal context). Work on "profiles" should be grounded in case studies of existing and proposed systems.
- RC/S4 - Work to support the standards activities in testing, validating, accrediting and accepting deployed systems at the hardware, algorithm and user acceptance levels.

7.5.2 FP6: BioSec (IST-2002-001766):

BioSec (IST-2002-001766) is an FP6 project (Integrated Project) that has tried to address some of the challenges outlined in the FP5 biometric roadmap. The project has sought to investigate 20 of the 38 research challenges of BioVision [2]. For example, the BioVision defined *RC/Sec 5: Systems and Design* highlights the need for *"Live and Well"* features in biometric systems.

BioSec has addressed this challenge with researching fingerprinting, iris, voice and 3D biometrics.

The project addressed evaluations of best-practice implementation methods, developed scenarios on physical and remote access, created a database on multimodal biometrics for the research community, and produced a combined speaker and speech recognition system. It has also advanced much-needed technologies such as 3D imaging and aliveness detection (to ensure an individual is not deceased or dismembered and that a photograph, model or recording cannot be used).

7.5.3 FP6: BioSecure, (IST-2002-507634)

BioSecure, (IST-2002-507634) is an FP6 project (Network of Excellence) that examined biometrics in terms of integrating multidisciplinary research efforts and evaluation methods with the aim of increasing trust in biometrics. Another core focus of BioSecure is the building of multimodal systems and definition of the state-of-the-art in different biometric classifications such as face and fingerprint recognition [4], [5], [6]. In reflection of the BioVision Roadmap, BioSecure mainly addresses "Trial, Testing & Legal", "Components" and "Standards".

7.5.4 FP6: SecurE-Justice (IST-2002-507188):

Another FP6 project that indirectly relates to the BioVision roadmap is called SecurE-Justice (IST-2002-507188). This project has biometric authentication aspects, whilst providing a high degree of security to communication and collaboration instruments used in everyday life by citizens and law enforcement officials involved, especially in penal trials.

The SecurE-Justice project will address the protection of all the actions and activities relating to the investigation of the crime, the collection of evidence (including witnesses and testimonies) and the questioning of suspects.

As part of this projects achievement, it will provide error free user authentication and authorisation via biometric 3D facial recognition [9].

7.5.5 FP6: Secure-Phone (IST-2002-506883):

Secure-Phone (IST-2002-506883) aims at enabling biometrically authenticated users to deal mobile contracts (m-contracts) during a mobile phone communication in a dependable and secure manner. The end users e-signature will be authenticated by comparing several biometrical features stored on the device SIM card. Similar to BioSecure, it will provide multimodal concepts with the innovative fusion and combination of different techniques such as voice verification techniques, face recognition techniques and handwritten Signature verification techniques [10].

Biometric authentication is the finishing link in the trust-chain, directly linking the authenticated individual to the secured communication channel. In a multi-modal scheme, the system has to decide if the request is granted or denied. Biometric data are analysed by expert algorithms, which give their numeric opinion on identity of the user.

7.5.6 FP6: Digital Passport (IST-2004-507974):

The Digital Passport project (IST-2004-507974) has set about developing the next generation digital passports. These passports will contain an IC microcontroller containing and processing cardholder's personal and biometric data. An RSA microprocessor will provide the support for PKI based security and capacity for encryption and digital signature. The solution is based around well defined standards such as ISO 7816-15, ISO 14443, ISO WG3.

7.5.7 FP6: HUMABIO (IST-2006-026990):

The HUMABIO project commenced in January 2006 and aims to develop a **modular, robust, multimodal** biometric **authentication** and **monitoring** security system. This will utilise a **biodynamic physiological profile**, unique for each individual, and advancements of the state-of-the art in behavioural and other biometrics, such as facial, speech, gait recognition and seat based anthropometrics. It also aims to create an enhanced security framework for the integration of the biometric authentication system to a **corporate security grid** or other **controlled and monitored ambient intelligence environments**. This will guarantee trust and privacy concerning the citizen's personal biometric template and data. This will include the introduction of new types of biometrics and implement emerging biometric modalities such as EEG baseline and Event Related Potentials. It also involves the introduction of novel sensors in the biometrics systems/market aiming at the user's convenience, system unobtrusiveness and the integration of biometrics to Ambient Intelligent solutions. It will involve a combination of the authentication mode, with validation of nominal physiological state and continuous physiological monitoring in order to boost safety levels for critical operations.

7.5.8 FP6: 3D-FACE (IST-2006-026845):

The 3D-Face project commenced in April 2006 and aims to explore multimodal facial data (3D, 3D+2D), face texture and multiple algorithms. It aims to improve biometric performance by addressing; FAR < 0.25%, FRR < 2.5%; internal competition of labs and selection of best results by independent evaluation. It will also explore template protection and privacy protection. It will investigate validation at airports, operational performance and social and operational issues. It will also examine standardization and any direct influence on international standards.

7.5.9 FP6: MIT (IST-2005-027351)

MIT (Minutiae Template Interoperability Testing) is an FP6 project that focuses on improving the state of the art in fingerprint biometrics. The current adoption of fingerprint data has used the fingerprint image methodology, but data sizes make this inefficient compared to the minutiae template used by most fingerprint systems. The use of minutiae based templates enables solutions to be more privacy sensitive, as the template can be stored easily on the memory restrictive smart cards. The project takes as its starting point the existing work on fingerprint minutiae data interchange standards, the problems of interoperability identified in the recent test for the seafarers ID card, and the current NIST benchmark of minutiae interoperability, and will extend this existing work to improve the standards, the test methods and the interoperability of fingerprint minutiae systems [68].

Overall MIT Objectives are to:

- Work with EC to provide for testing and certification define criteria for interoperability testing
- define criteria for interoperability testing
- develop a database of fingerprint images to enable testing
- develop a test bed enabling the automated and repeatable testing of fingerprint minutiae interoperability, and also investigation of how factors such as image quality are important for interoperability
- incorporate an improvement step, whereby the interoperability of the tested systems can be improved, and
- provide for the testing of interoperability of future systems from further vendors.

Scientific Objectives of MIT:

- The first objective of the MIT is not only to test if interoperability is achievable, but to conduct effective research and progress to deliver encoding algorithms which are able to provide interoperability
- The second major objective of this project is to deliver a framework and a certification process which allow future interoperability. It is envisioned that an independent certification laboratory will conduct such tests.

One of the main challenges highlighted by MIT is [69]:

- Current state-of-the-art has many interoperability problems within the biometric arena that need to be resolved.

Testing and improving the state-of-the-art on fingerprint minutiae biometrics is important.

7.6 References

[1] Mark Rejman-Greene, "BioVision Research Challenges", 2003, www.eubiometricforum.com

[2] "BioSec and Biometric Research Challenges", www.eubiometricforum.com

[3] BioSecure: www.biosecure.info/

[4] J. Kittler et al, "State of the art in multimodal biometric systems", Deliverable D8.1.1.

[5] Massimo Tistarelli et al, "Report on the face state of the art", Deliverable D7.2.2.

[6] Raymond Veldhuis, "Report on the fingerprint state of the art", Deliverable D7.3.2.

[9] SecurE-Justice Brochure: www.secure-justice.org

[10] Secure-Phone: www.secure-phone.info

[11] Tanja Lange et al, "Open Problems in Cryptology", Deliverable D6 V2.1, 2003.

[12] Tanja Lange et al, "Research Agenda for the Future of Cryptology", Deliverable D5 V2.1, 2003.

[13] Ecrypt: www.ecrypt.eu.org

[14] Ecrypt STVL-WG3: http://www.ecrypt.eu.org/stvl/groups.html

[15] Anne Canteaut et al, "Ongoing Research Areas in Symmetric Cryptography", Deliverable DSTVL.4, 2006.

[16] Louis Goubin etal, "New Technical Trends in Asymmetric Cryptography" Deliverable D.AZTEC.3, 2005.

[17] Nigel Smart et al, "Provable Security:Designs and Open Questions", Deliverable D.AZTEC.1, 2005.

[18] Giuseppe Persiano et al, "Second Summary Report on Two-Party Protocols",Deliverable D.PROVI.4, 2006.

[19] Berry Schoenmakers et al,"Second Summary Report on Multiparty Protocols", Deliverable D.PROVI.5, 2006.

[20] Jesper Buus Nielsen et al, "Second Summary Report on Unconditionally Secure Protocols", Deliverable D.PROVI.6, 2006.

[21] Elisabeth Oswald et al, "State of the Art in Hardware Architectures", Deliverable D.VAM.2, 2005.

[22] Elisabeth Oswald et al, "State of the Art in Hardware Implementations of Cryptographic Algorithms", Deliverable D.VAM.10, 2006

[22] Francois-Xavier Standaert et al, "Electromagnetic Analysis and Fault Attacks: State of the Art", Deliverable D.VAM.4, 2005.

[23] Elisabeth Oswald et al "Hardware Crackers", Deliverable D.VAM.3, 2005.

[24] UVIGO, CNRS, "Second Summary Report on Fundamental Aspects of Watermarking Schemes", Deliverable D.WVL.8, 2006.

[25] UNIGE, "First Summary Report on Practical Systems", Deliveable D.WVL.3, 2005.

[26] Martin Schmucker et al, "First Summary Report on Forensic Tracking", Deliverable D.WVL.7, 2005

[27] Jana Dittmann et al, "Audio Benchmarking Tools and Steganalysis", Deliverable D.WVL.10, 2006.

[28] Jan Huizenga et al, "Roadmap for Advanced Research in Privacy and Identity Management", Deliverable RD 2.2, 2003.

[29] FIDIS: http://www.fidis.net/

[30] Matthias Bauer et al (eds.), "Structured Overview on Prototypes and Concepts of Identity Management Systems", Deliverable D3.1, 2005.

[31] Mark Gasson et al (eds.), "A Study on PKI and Biometrics", Deliverable D3.2, 2005.

[32] Günter Müller et al (eds.), "Study on Mobile Identity Management", Deliverable D3.3, 2005.

[33] Marit Hansen et al (eds.), "Privacy and Identity Management for Europe – PRIME White Paper V1", Deliverable 15.1, July 2005.

[34] Simone Fischer-Hübner et al (eds.), "Framework V1", Deliverable D14.1.a, June 2005.

[35] Simone Fischer-Hübner et al (eds.), "Framework V0", Deliverable D14.0.a, June 2004, revised version June 2005. [36] Marcelo Masera et al, "A Dependability Roadmap for the Information Society in Europe Part 1 – An Insight into the Future", Deliverable D1.1, August 2003.

[37] Marcelo Masera et al, "A Dependability Roadmap for the Information Society in Europe Part 3 – Towards a Dependability Roadmap", Deliverable D1.1, August 2003.

[38] Marcelo Masera et al, "A Dependability Roadmap for the Information Society in Europe Part 2 – Appraisal of related IST Roadmaps", Deliverable D1.1, August 2003.

[39] Bob Hulsebosch et al, "Initial Dissemination Plan", Deliverable D6a, August 2002.

[40] Bob Hulsebosch et al, "Final Roadmap (extended version)", Deliverable D4, 2003.

[41] Marek Rejman-Greene, "BIOVISION Final Report", Deliverable D1.4, July 2003.

[42] "TIRAMISU: The Innovative Rights and Access Management Interplatform SolUtion", White paper.

[43] Zvi Lifshitz, "TIRAMISU's DRM Requirements", INTERNET STREAMING MEDIA ALLIANCE, 2004.

[44] Philips et al, "Watermarking applications and requirements for benchmarking", Deliverable D2.1, 2000.

[45] "RESET Roadmap 5.0 Roadmap for European research on Smartcard rElated Technologies", Deliverable D5, May 2003.

[46] Mosquito Website Resource: http://www.mosquito-online.org

[47] SecurIST, "Convening's of the Task Force – Report of the 2nd Workshop", April 2005

[48] Jan Camenisch (ed.), "Annual Research Report I", Deliverable D16.1.a, April 2005.

[49] Jan Camenisch (ed.), "Annual Research Report II", Deliverable D16.1.e, April 2006.

[50] S3MS Website: http://www.s3ms.org

[51] SecurIST "Convening's of the Task Force – SecurIST & IST Call 4 Projects Integration Workshop report", Deliverable D2.2, March, 2006

[52] FASTMATCH Website: http://www.fastmatch.org/

[53] FP6-IST Programme, "R&D Projects in the Strategic Objective "Towards a global dependability and security framework", 2006

[54] SERINITY Website: http://www.serenity-project.org

[55] IRRIIS Website: http://www.irriis.org/

[56] CRUTIAL Website: http://crutial.cesiricerca.it/

[57] HIDENETS Website: http://www.hidenets.aau.dk

[58] GRID Website: http://grid.jrc.it/

[59] CI2RCO Website: http://www.ci2rco.org/

[60] DESEREC Website: http://www.deserec.eu/

[61] DAIDALOS Website: http://www.ist-daidalos.org/

[62] ESFORS Website: http://www.esfors.org/

[63] SECOQC Website: http://www.secoqc.net

[64] UbiSec&Sens Website: http://www.ist-ubisecsens.org/

[65] ReSIST Website : http://www2.laas.fr/RESIST/

[66] **Development of secure and robust watermarking algorithms.** http://cordis.europa.eu/fetch?CALLER=FP6_PROJ&ACTION=D&RCN=78378&DOC=15&CAT=PROJ&QUERY=1151928191355

[67] POSITIF Website: http://www.positif.org

[68] MIT Website: http://www.mitproject.com/

[69] Porvoo Website: http://porvoo9.gov.si/MIT_Presentation_vs_31-3-2006.ppt

[70] SEINIT Website: http://www.seinit.org/

[71] Michel Riguidel et al, "Assessment of threats and vulnerabilities in networks", Deliverable D1.2, 2004.

[72] Clarke, J. Howker, K. et al., “Joint SecurIST, Mobile and Wireless Workshop report”, May 2006, www.securitytaskforce.eu

[73] Lechner, S. et al., “SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework”, Issue 2.0 June 2006.

[74] Naqvi, Syed, et. al., “Joint SecurIST, Mobile and Wireless Workshop report”, May 2006, www.securitytaskforce.eu

[75] Trust In the Net Workshop (09 Feb. 2006) report available at http://www.egov2006.gv.at/Reports/Report_Trust_in_the_Net_Vienna_09_FEB_06.pdf

8 Annex III – EU Security and Dependability Task Force (STF) detailed outcomes.

Table of Contents

8.1 Introduction

The Security and Dependability Task Force was formed with the intention of providing the views of the researchers themselves on the most important and critical areas for future research priorities in their areas of expertise. The following sections give a description of the Task Force initiatives that were established, together with the results from the various workshops and consensus gathering activities within the STF that provided further focus and prioritisation of the extensive list of identified issues. These results were submitted to the SecurIST Advisory Board for their consideration, and have been used as input to this report. The relationship between the STF results and the Advisory Board's recommendations is explored fully in Annex IV, below.

8.2 Cryptology and Digital Asset Management Research Projections

It was decided by the STF members to have a dedicated Cryptology Research Initiative (CRI) and a Digital Asset Management Initiative because the two areas were each quite wide, and both were considered to be of considerable importance and scope.

8.2.1 Cryptology Research Initiative (CRI)

The Cryptology Research Initiative (CRI) is focused on advanced and novel cryptographic algorithms and protocols and techniques for watermarking and perceptual hashing techniques. The goals are to improve security and confidence in these techniques, to develop secure and efficient implementations and to integrate these techniques into advanced applications such as electronic voting, fighting spam, and privacy enhancing technologies.

The initiative has drawn on the experience of past and previous projects such as ECRYPT along with other areas of expertise in Europe to draw its conclusions of where the future focus of security should lie.

Hence, the CRI has identified a number of key challenges that should be a priority in FP7:

CRI 1. Cryptology in an ambient intelligent world. As we evolve towards an ambient intelligent world, and privacy concerns will increase, cryptology will need to be available everywhere – even in the smallest devices. In this context, cryptology will be needed that can offer acceptable security and performance at very low cost (hardware footprint, power consumption). The importance of "distributed trust" (or secure multi-party computation) will grow in order to reduce dependency on any single node – "you can trust this because you don't have to".

CRI 2. High Performance algorithms for authenticated encryption. High performance algorithms for authenticated encryption will be needed to deal with communication speeds and storage size that are both growing faster than the speed of processors. Some of the storage applications need cryptographic techniques that offer long-term security for long highly sensitive data (50-100 years). This also includes the developments of new algorithms that offer stronger resistance against mathematical advances and even quantum computers.

CRI 3. Advanced crypto techniques for media protection. This challenges includes Advanced crypto techniques for media protection (authentication, copy protection/detection, perceptual hashing, Zero Knowledge watermarking and fingerprinting).

Digital Assets Management Initiative (DAMI)

It was decided after consultation with the members of the CRI and the Executive board of the STF that since the subject area of Digital Asset Management was so important and complex, that there should be an initiative specifically to cover the challenges for the area digital asset management. The members of the DAMI have identified a number of key challenges that should be a priority in FP7.

DAMI 1. Development of secure and robust watermarking algorithms. Digital watermarking, i.e. the possibility of imperceptibly and indissolubly attaching a piece of information to a hosting digital asset such as a video, a still image or an audio file, has been proposed as a viable solution to several security problems related to the way digital assets are handled in our digital age. The addressed problems include ownership verification, copyright protection, tracing of illegal uses and/or non-allowed redistribution etc … The initial enthusiasm about watermarking technology froze soon when researchers realized that the security and robustness requirements set by practical applications were very difficult to fulfil. Yet, digital watermarking remains one of the few solutions (in some cases the only solution) advanced so far to enforce digital rights managements legislations in highly non-structured scenarios.

The main challenge researchers are still facing regards the development of a watermarking system that is robust against the several manipulations digital assets may undergo during their life cycle, and secure against any explicit attack against it brought by a malevolent third party usually termed pirate or attacker. In the last few years important advances have been made towards the definition of a general theory of watermarking robustness and security that can be used: a) to set the ultimate limits of watermarking technology; b) to rigorously measure the security of a watermarking system; c) to compare different systems from a security perspective. Yet, the development of a watermarking scheme that is at the same time secure and robust is still an open issue, possible the most crucial one, for which an answer will have to be searched in the next few years.

DAMI 2. Asset authentication through intrusive (watermarking) and non intrusive (digital forensics) techniques. Authentication of digital data has been traditionally addressed by means of cryptographic primitives, such as digital signatures and hashing. Such techniques, though, guarantee the perfect integrity of electronic documents since authentication fails if even a single bit is altered. Such a strict definition of authenticity is not always appropriate for multimedia data where there is an interest in permitting some alterations that retain the perceptual meaning of the original content. Furthermore, when a prohibited alteration is made, it is desirable to not only detect that a change has occurred, but to also identify where in the document the change is, and possibly to have at least an idea of which the original content was.

The techniques proposed so far to deal with asset authentication can be split into two fundamental groups: invasive and non invasive techniques. According to the former approach, authentication is achieved by first inserting within the to-be-protected asset a digital watermark whose presence and integrity is later on taken as evidence of authenticity; the latter approach belongs to the wider class of digital forensics techniques, and tries to acquire authenticity evidence *a posteriori*, without altering or damaging the original, for example by relying on the intrinsic and singular noisiness of acquisition devices (e.g. the ccd array of digital cameras).

In both cases the development of advanced techniques permitting to discriminate between allowed and non-allowed manipulations, e.g. between manipulations that does not alter the semantic content of the to-be-authenticated document and does altering it, is an active research topic for which efficient solutions will have to be found in the years to come. Authentication security will have to be addressed as well.

DAMI 3. Asset identification: perceptual hashing. An essential ingredient in any secure multimedia application is unambiguous document identification. Besides the techniques that are known from computer science, that being bit-wise precise do not fit the nature of multimedia assets, two main approaches are currently being put forward being more focussed on signal processing and perceptual aspects. The best known of these methods is digital watermarking and is addressed by challenge 56. The second method is known under a set of different names such a perceptual hashing and perceptual fingerprinting. This method is characterised by the extraction of perceptually robust features (in analogy with human fingerprints) that uniquely characterise the content of the to-be-identified document. Despite the good opportunities offered by the perceptual hashing approach to identification, two fundamental questions have to be answered before perceptual hashing can be effectively used in practical applications: Which are the perceptual features that could better serve the purpose of data identification? What is the sensitivity of the human senses with respect to such features? This simple formulation hides very difficult problems due to the fact that perception is a very complex process involving sensory mechanisms of different levels. Other hot challenges in this field regards: a) the derivation of theoretical bounds on fingerprint size; b) the relation between fingerprint and quality; c) the benchmarking and comparison of different identification systems.

DAMI 4. Conditional access to the digital assets. Another essential ingredient of any secure asset management system is the possibility of restricting the access to the digital assets, or part of them, to authorized users. Whereas cryptographic techniques are an obvious solution, the interplay of encryption and signal processing must be carefully considered. In order to allow a secure, fast, and flexible access to the digital assets, it is in fact fundamental that the cryptographic primitives are adapted to, or, even better, jointly designed with the asset format. This is the case, for example, of secure access to coded data, e.g. a compressed video or audio file. Being the encryption of the whole bit stream unfeasible for complexity reasons, it is necessary that only some critical parts of the stream are encrypted, without loosing security or coding efficiency. At the same time it may be desirable that the partial encryption of the bit stream does not prevent a flexible access to the coded data, e.g. it should allow fast forward and backward playing modes and fast searching. Finally, different users may be allowed to access different parts or different quality levels of the digital assets according to their rights, thus calling for multi-level encryption. Reaching all the above goals simultaneously is a very complex task that is better addressed if coding and encryption are performed jointly.

DAMI 5. Asset processing in the encrypted domain. Most of the currently available technological solutions for "secure manipulation of signals" simply try to apply cryptographic primitives in order to build a secure layer on top of the signal processing modules, able to protect them from leakage of critical information. When cryptography is used as a module operating separately from the signal processing part of the application, we typically have to assume that the involved parties or devices trust each other, and that the cryptography layer is used only to protect the data against third parties not authorized to access the data or to provide authenticity. In many cases, though, this is not the case, since the owner of the data may not trust the processing devices, or those actors that are required to manipulate them. This may result in a lack of security of the overall system. It is clear that the availability of signal processing algorithms that work directly on encrypted data would be an invaluable help for application scenarios where "valuable" signals must be produced, processed or exchanged in digital format.

Whereas the development of tools capable of processing an encrypted signal may seem a formidable task, some recent, still scattered, studies, spanning from digital watermarking, through secure compression, and access to encrypted databases, have shown that the application of signal processing in the encrypted domain is indeed feasible. Though promising, these studies are of an embryonic nature, hence many open questions about the potentiality and limits offered by the application of signal processing tools operating securely on encrypted data need to be addressed.

While it is immediate to recognize the difficulty of the problems on the ground, it is easily understood that their, even partial, accomplishment would lead to the foundation of a new interdisciplinary research field, with a profound impact on the way we process, store and communicate multimedia data.

DAMI 6. Covert Communications (steganography and steganalysis). Another key issue is the possibility of establishing a covert communication channel by means of steganographic tools. Whereas one may wonder about the legitimacy of this action, it is clear that the existence of a covert channel between two parties wishing to communicate would be of great help to protect the privacy of the communication and the anonymity of the participants. On one side this can be a desirable feature in our age where any of our actions may be easily monitored without our explicit permission. On the other side, it may be the case that the covert channel is used for malicious purposes, e.g. terrorist activity. For this reason, reliable and accurate detection of covert communication could prove vital in the future as the society creates defence mechanisms against criminal and terrorist activities. Fast and reliable identification of stego media objects and estimation of the secret message size and its decoding are among the highest ranking requirements formulated by law enforcement.

8.3 Identity and Privacy Management Research Projections:

8.3.1 Identity and Privacy Initiative (IPI)

An Initiative within the STF was established entitled the Identity and Privacy Initiative (IPI), which addresses research focusing on digital identity management, privacy protection and mediation, personal data environments and the development and use of privacy-enhancing technologies, (self-) management of privacy, as well as privacy and authentication mechanisms within fixed and mobile/wireless network environments.

The members of the IPI have identified a number of key challenges that should be a priority in FP7.

IPI 1. Potential unforeseen risks with the unauthorized or unintended use of computerized personal identity information will increase. One of the major challenges in collecting personal data at various points of contact is how to be sure that the data is treated according to the requested security and privacy standards and how anyone can assure that the data is only used for the intended purpose. In that respect, key issues in the future will not only comprise how to treat individual data that have been collected and processed for a specific purpose, but also include how combining of data on an individual to derive an own profile can be managed. Such a profile may make the “traditional” ID concept obsolete. It remains to be seen how profiled individuals will respond if this data set is false or if it is misused. New technologies or services may also lead to new risks to privacy: In many cases additional data is processed - sometimes only because of a naïve implementation without the real need for those data. Often the processes are performed seamlessly which may be good for convenience of use, but also means that most users are not fully aware about what is exactly happening and whether and how their private sphere is affected. Examples are location-based services or systems in the field of ambient intelligence which may release and transfer personal data without knowledge - and, hence, without consent - of the individual.

IPI 2. Qualification of numerous new identification methods and new identity management systems. Another key challenge will be on how to qualify new identification methods and new identity management systems for providing secure, reliable and privacy-enhancing ways to process personal data. The compatibility of these systems across technologies and across different countries will also have to be evaluated. Especially in the field of biometrics it is not fully clear which side effects may occur, e.g., what medical data could be extracted from the biometric raw data of the individual or accordingly the biometric templates. As part of a first comparison of different identity management systems, deficiencies have been found concerning the privacy and security functionalities of these systems which are also typical for other ICTs. For example:

The standard configuration rarely addresses privacy functionalities sufficiently.

Furthermore, people are not or at least not enough encouraged to utilize their privacy rights such as access, correction of data, deletion, withdrawal of consent etc. Technology could better support such privacy control functionality.

Many technical systems dealing with personal data do not generate digital evidence which can be used to enforce a right and which is also accepted before court.

Additionally, many of the systems today do not have sufficient protection mechanisms in place to prevent identity theft.

All this applies to ICT systems for both the actual data processing entity and the individual who the data belongs to. One of the reasons for all these shortcomings is that not all systems are built on an overall and committed standard. Trustworthy computer systems and infrastructures are still missing. Thus, there is a lot of research work to be done on the future of identity management systems and their contribution to privacy.**IPI 3. Development and integration of Privacy-enhancing Technologies (PETs) into ICTs.** Solutions to the aforementioned problems can be implemented by privacy-enhancing technologies (PETs)[15], which should enhance the state-of-the-art of ICTs (i.e. dominant on the market and in use in organizations) with respect to at least some properties related to privacy or informational self-determination. It is recognised that they themselves span another complex of challenges.

Many building blocks for PETs have already been developed, but only few of them are available on the market until now. Thus, successful business models for PETs and for supporting infrastructures have still to be elaborated.

As PETs will need to be integrated within an environment, there may be interactions and interdependencies with other system components, which influence security and privacy. This will require a certain degree of redesign within the system components. Even a combination of multiple PETs may lead to weakening rather than enhancing the degree of privacy. Clear privacy metrics are missing. Also, an analysis of possible interdependencies between the use of PETs and other technological components and of related effects on the users' privacy does not exist, let alone ways to inform them appropriately. Such information would help to know additional precautions that a user has to take in order to assure his or her privacy. Privacy seal programs and audit programs for example should take into account that assumptions on the environment and its trustworthiness should be communicated to and understood by the users.

8.4 Dependable & Critical Infrastructure Research Projections:

There were quite a number of Initiatives within the Security and Dependability Task Force covering these areas of research. These include the Dependability and Trust Initiative (DTI), Security Policy Initiative (SPI), Security Research Initiative (SRI), IPv6 Initiative (V6SI), the Security Architecture and Virtual Paradigms Initiative (SVPI), Internet Infrastructure Security Initiative, the Applications Security Initiative (ASI) and the Methods Standards Certification Initiative (MScI).

8.4.1 Dependability and Trust Initiative (DTI)

DTI is concerned with two main issues: the confluence between classical dependability and security, met essentially but not only by the concept of common 'accidental fault and malicious intrusion tolerance'; and the necessary but often forgotten link between trust (dependence or

[15] In this document, we use the term PET in a broad sense, comprising all privacy technologies which enhance the state-of-the-art (i.e. dominant on the market and in use in organizations) with respect to at least some properties related to privacy or informational self-determination.

belief on some system's properties) and trustworthiness (the merit of that system to be trusted, the degree to which it meets those properties, or its dependability).

The members of the DTI have identified a number of key challenges that should be a priority in FP7. These include:

DTI 1. Trustworthy adaptability.

(i) complexity of systems is growing out of control, amplified by the advent of ambient-intelligent pervasive and ubiquitous computing; more and more "always-on" complex systems are being deployed or planned, especially by governments;

(ii) growing interdependencies between systems, services and humans;

(iii) threats take advantage from complexity and interdependencies;

(iv) as in nature, this requires adaptation towards a state good enough for survivability.

It is a challenge/priority theme because:

It requires innovative approaches such as proactive-reactive design under uncertainty, adapting functional and non-functional properties while providing guarantees on adaptation result, autonomous and decentralised system algorithmics, trustworthy monitoring and update for continuously-on systems.

If addressed, this will contribute towards the widespread deployment of very dynamic and evolvable systems that can be trusted in spite of their complexity. In other words, where ‘complexity’ is not an excuse for ‘undependability’ as is the case today.

If not addressed, there are a number of risks including a serious fallback on plans to realize the ambient-intelligent society; serious hazards in the operation of systems that alternate between states of fossilised dependability/security and periods of undependability/ insecurity during and after system changes.

DTI 2. Balanced trustworthiness

(i) various attributes of trustworthiness (reliability, security, safety, etc.) extremely difficult to estimate and predict;

(ii) attributes emerging from combinations thereof, even harder.

(iii) on the other hand, the perception of trustworthiness and hence the degree of trust may vary depending on which side of the fence we are in (e.g. DRM, TCPA).

Is a challenge/priority theme because:

- Achieving effective trade-offs between these is often required but unfortunately is a continuing even greater challenge.
- Trade-offs between attributes (ex. availability and integrity, security and dependability), and trade-offs between what suppliers and users seek (e.g. privacy, control, etc.), are at the heart of this problem.

If addressed effectively it will:

- help answer questions like "How hard can we make it for a hacker to attack a system, and still keep the service price/usability attractive to a legitimate user?".
- enable the provision and deployment of much more satisfactory systems and services.

If not addressed, risks:

- Technologies deployed will risk becoming part of the problems, rather than the solutions.
- Systems approach to dependability will continue the road of patchwork, unfortunately seen far too often.

- A continuation of the present situation in which many systems provide a very poor balance of the attributes, e.g. high security at a great cost to usability.

DTI 3. Rethinking availability

Description:

(i) Classical dependability based on aprioristic and all-or-nothing criteria. Availability has been designed-in by redundancy according to forecasted fault modes, and predicted/ contracted to the user upon deployment. (ii) Whilst remaining a crucial attribute of today's systems, the future will bring new variables that will invalidate this status-quo: dynamics, uncertainty, evolvability, mobility, energy, maliciousness, sharing of critical and non-critical operations.

Is a challenge/priority theme because:

This requires an approach where availability becomes itself an evolvable and survivable attribute, in essence conditioned by: evolution of the environment; oscillation in QoS of the infrastructures. However, guarantees must still be met in some form, and this is a hard research problem, encompassing technology and societal factors (such as managing user expectations).

If addressed will:

- Bring in a totally new perspective on the 24x7 problem equation in a world of threats, what we might describe as 'acceptable availability'.
- Hopefully contribute to creating future infrastructures that are at least as resilient to crashes, overloads and attacks as today's systems are.

If not addressed, risks:

- Keep increasing the risk of operation of the current combined critical/non-critical infrastructure substrate.
- Amplify this risk by extending it to edges brought in by ambient intelligence, like sensor nets, mobile gadgets, home networks, car communication, navigation assistance systems, etc.

8.4.2 Security Policy Initiative (SPI)

The SPI aims to identify critical issues towards the creation of a policy-based security management system, including also techniques and tools for security design and technical-economical simulation of the effects of a policy.

The members of the Security Policy Initiative (SPI) have identified a number of key challenges that should be a priority in FP7. These include:

SPI 1. Security Analysis. Following the idea that "you can't control a system if you can't predict its behaviour", automatic security analysis methodologies and tools need to be developed. This must be focused towards predicting differences in behaviour of an attacked system. It must consider system functionality and performance, and must be able to generate not only technical data but also economical parameters (such as estimated loss per minute caused by a specific attack).

The latter is very important to reconcile investment with potential damage and lays the foundation for the development of ICT risk insurance strategies. Moreover, international agreements already call for quantitative economical evaluation of ICT risks (e.g. the Basilea-2 agreement) and this will increasingly be the case in the future.

Security analysis should be performed via system simulation and formal methods. There is not a clearly superior approach among them, and both should therefore be pushed because they are capable to catch different aspects of the security problem. Moreover simulation and formal methods may differ in the size of the manageable problem, and can also be used iteratively to validate each other's results.

If effective security analysis techniques (be them based on simulation or formal methods) are not developed then we will be unable to predict the effectiveness of our security solutions perform and to perform a cost-benefit analysis. In other words, we'll continue to have qualitative analysis, rather than quantitative.

SPI 2. High Level Policies. Since "you can't design/configure a system if you can't exactly express your needs", we call for the capability to describe and manipulate high-level security policies. This is opposed to the current situation where security requirements are very vague, expressed in natural language and translated to the actual configuration of the protection tools by security technicians. On the contrary, a high-level language should be more close to individual needs and business logic, so that it can be adopted by final users (either citizens or ICT managers) to clearly state their protection requirements. Appropriate tools must then be developed to automatically refine the high-level policies into low-level security controls (security management). This in turn generates the issue of keeping the high and low level views synchronized, since day-by-day management tools typically work at the lower levels and could invalidate the design automatically generated from the high-level policies. Policies are also vital in cyberspace interactions, such as those that occur in P2P systems or e-commerce transactions, to automatically negotiate acceptable policy (and hence, a set of security parameters) with neighbours and the intelligent ambient.

If a high-level policy system is not developed, then the protection systems will be prone to design errors (due to bad specification), difficult certification and audit, and complex interaction in open environments.

SPI 3. System Modelling. Following the concept that "you can't protect a system if you can't describe it", it is required to develop models of the target system and the surrounding ambient, including users and applications. The description must include the system topology, the network and application functionality, the security capabilities and the user behaviour. Integration with existing partial views of the system (such as that used for network management and for inventory control) is important, as well as the ability to accommodate dynamic changes (for example of network filters or routing strategy). System model is vital to perform security analysis (SPI challenge #1) and to automatically deduct and implement controls specified by high-level policies (SPI challenge #2). In other words, it is the foundation to build automatic security management techniques. Moreover a correct system model, that includes security capabilities, is also relevant to any negotiation strategy when an agreement has to be found about protection parameters with neighbours and the ambient in general.

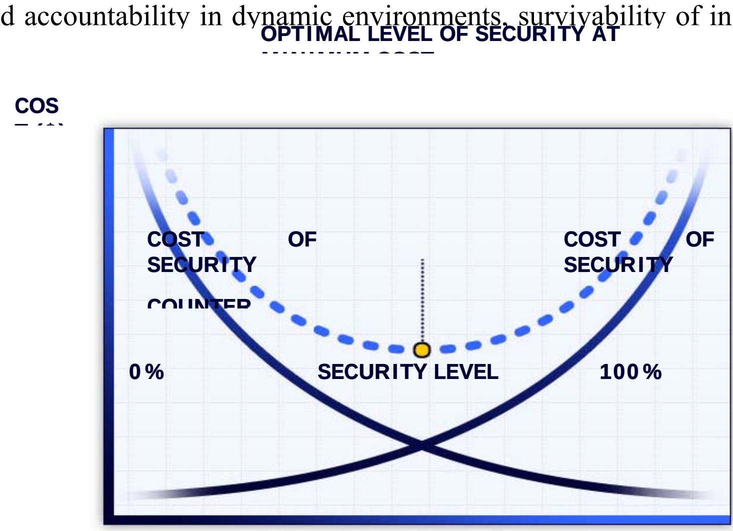
If comprehensive system description capabilities are not developed, then we will lack the substrate for all the other activities and in particular we will be unable to perform rigorous quantitative work, be that related to security analysis or to automatic policy deployment.

SPI 4. Neutral Security Capability Language. The top-down approach foreseen by the SPI could underperform if the protection tools used to implement the policy do not provide a full description of their capabilities, or if they use specific concepts or tools invented by a provider. To solve this problem, a neutral security capability description language should be created and security tools could provide proper hooks to implement some high-level functions without disclosing their proprietary or patented solution.

8.4.3 Security Research Initiative (SRI)

This initiative is engaged in linking results of different research groups and initiatives into one cohesive vision for the European research and development strategy addressing security and privacy in ICT such as innovative network security architecture and models, new protocols for

identification and authentication of nodes, services, routes, active code, etc. as well as for distribution of credentials, coping with new attack models such as distributed denial of service attacks, multi-party security association management, issues related to management of sources of trust and accountability in dynamic environments, survivability of infrastructures, including
on
in
to
de
of
re
an
he
ut
nd
or
networks vary. However, from the user perspective, they will need to be able to get end to end security and trust through interoperable networks and functions. Hence, number of challenges identified in the above sections addressing different initiatives form part of overall challenges to be addressed as security research framework, addressed by SRI.



SRI 4 (with input from IPI) Usability. (IPI) A general problem of today's Security tools is that they may be too complex for most of the users, especially with regard to Privacy Enhancement Technologies. This is related to the fact that the complexity of legal regulations on privacy and of ICTs themselves has grown over the last years. Thus, reduction of complexity and enhancement of usability play an important role for their distribution. In particular, it is an unresolved problem until now to determine the best ways to impart an integrative view on the private sphere of the individual and to support the user in making decisions concerning the release of personal data. Here, not only technologies may be employed, but also the service of other parties can help in this matter, e.g. by providing appropriate configuration files or by acting as intermediaries on behalf of the user if desired. E.g., in the security field there is a good tradition of Computer Emergency Response Teams (CERTs), which inform about security incidents and the countermeasures that have to be taken. People may need additional organizations, which inform them about "privacy incidents", i.e. events, which may affect their privacy, and give advice how to react in order to maintain their private sphere. As acceptance and user-friendliness of PETs is important, appropriate user models and user interfaces should be elaborated.

(SRI) Usability of security features developed and built into the system are the key factors in providing the user with the control of security and privacy and for his data protection. This issue is not well addressed (or not even considered) by the vendors and service providers. The challenge is to understand user behaviour in the contextual environment and provision appropriate measures.

SRI 5. Cost Effectiveness. As depicted in the figure below, cost effectiveness of security and trust is another key challenge, which balances the level of security that can be provided at the reasonable cost. The security and trust of ICT is always related to the business risk assessment. Optimisation between the costs and security measures has to be managed.

Figure 9 – Balancing **C***osts* vs. *Security Level*

SRI 6. Citizen empowerment. In many cases, users themselves will have to manage their privacy preferences. They should be supported by technologies for self-management (among others: identity management systems), which empower them to assert their rights. The inclusion of "privacy control functionalities" such as negotiating privacy preferences, managing the consent, access and even correct or delete individual data processed by the data processing entity according to the applicable laws would enhance ICTs tremendously.

The field of ambient intelligence needs solutions for the informational self-determination of individuals, i.e., providing all necessary information and choices with respect to one's private sphere. How to achieve multilateral security in ambient intelligence is an open issue especially because personal information may be transferred to devices the trustworthiness and security of the device is not known and often times questionable. In these cases classic PETs and "privacy control functionalities" are lame ducks. We need new mechanisms that ensure that personal information continues to be protected once it has been given away.

SRI 7. Legally compliant systems. Designing legally compliant ICT systems is a challenge as well, especially in an international context with potentially numerous regulations, which even may be contradictory. Changes in legal regulations, as e.g. announced in the area of data retention, lead to updates or even redesigns of ICT systems. In particular where privacy law or privacy principles are affected, a careful development is necessary, e.g., to balance the demands of privacy and law enforcement. For biometrics, a careful evaluation of methods for verification or identification with respect to privacy is still necessary. In particular, side effects such as the possibility to disclosing medical or other unnecessary data for authentication purposes has to be elaborated.

The possibilities of authorized law enforcement access to data by law enforcement officials need to be developed in a way that minimizes the invasion of privacy and guarantees the individual's privacy principles. For instance, monitoring should be done on an isolated-case level rather than for all users of a system. Similarly, surveillance and monitoring methods, e.g., for criminal incidents, have to be developed, which are not privacy-invasive for individuals not involved in the recorded incident.

SRI 8 (input from IPI). Creating awareness

(IPI) Research should be conducted on metrics of privacy, which not only help in estimating the degree of privacy implemented within an ICT system, but also can be used to illustrate privacy-relevant parts and risks in PET user interfaces. False, incomplete or imprecise data including derived profiles and scoring values which are interpreted to predict the future of an individual may be an own focal point within this field.

Socio-economic factors should be investigated as well, e.g., in developing business models or performing acceptance studies. Best practice cases for PET building blocks such as convertible credentials should be elaborated.

In addition, psychological and sociological research should be performed for privacy, e.g., to get a better understanding on what motivates people to release data and to give better feedback to European citizen on the consequences of data released. Prototypes in the communication area are useful for users to experience the consequences, as giving away data here often results in more incoming communication (e.g. emails or other messages). So users can get a quick feedback with respect to their choices and the consequences.

By following these approaches, the goal of improving the business position for ICT companies in the EU will be reached by building trust and user acceptance. We are envisioning data protection features and the usage of PETs as a quality "trademark" for ICT solutions in Europe, which can also be used for supporting the export of European solutions.

The main objective is to enhance the image of the ICT development processes (and ultimately of the solutions) by integrating secure identity management and data protection mechanisms already in the design process of ICTs ie. data privacy by design.**SRI 9 (input from IPI). Behaviour of people with regard to Security and Privacy. (IPI)** There are considerable differing views on the user's perception and level of importance for privacy protection in situational settings. There have been studies in which the respondents rate privacy with highest importance, but, on the other hand, there are a lot of reports and observational studies that show how easy people give away their personal data without a second thought. Sometimes people are surprised and astonished about the amount of personal data that has been collected and stored about them. Research on the motivational factors behind this "irrational" behaviour would help ICT developers to build in expected and assumed privacy functionalities.

IPv6 Security Research Initiative (V6SI)

This initiative is highlighting the elements of IPv6 technology, which contains features that enable Internet users and commercial network operators to enhance the security and privacy of their networks. The members of the v6SI have identified a number of key challenges that should be a priority in FP7. These include:

v6SI 1. ***Dependence of the deployment of IPsec supported by a PKI infrastructure***. Similar to IPv4, IPv6 will depend on good deployment of the PKI Infrastructure.

v6SI 2. ***Motivational aspects of security vendors.*** The second challenge is the motivation of security vendors to move to deployment of IPv6 which would require redesign of de-perimetarisation of the firewall concept. This effort requires a solid business case.

v6SI 3. ***Acquisition of New security knowledge.*** The third challenge resides in the acquisition of new security knowledge to enable security engineers to write new lines of code that need to be tested and smoothly integrated into production networks without introducing new vulnerabilities. The perception that IPv6 is not a security panacea adds more to the fear and resistance to try new security concepts. IPv6 cannot indeed protect against misconfiguration, poor application design or poor security design. It cannot remove the need for vigilance and a pro-active approach to network security. However, IPv6 can help to raise the baseline of security for networks today. IPv6 technology can improve enterprise security, thereby protecting revenue. It can improve the security of public access networks, like Wi-fi hotspots, thereby minimising outages and customer dissatisfaction. IPv6 can provide better communications privacy than IPv4. The efficiency and security of IP mobility deployments can be improved with MobileIPv6, thereby reducing costs for operators. IPv6 can also minimise exposure to port scanning providing defence-in-depth and further protecting revenues and investments for both operators and end-users.

8.4.5 Security Architecture & Virtual Paradigms (SVPI) challenges

This initiative is examining the important aspect of virtualisation including exploring socially intelligent architectures for best value ubiquitous management of the dynamic Security & Trust (S&T) chain across time, place and space; end-to-end. This research area involves architecting the semantic representation of communicating domains and their enclosures to allow S&T services selection, composition and matchmaking. This entails providing adaptive and personalised protection for each entity through distributed management and delegation of security protection to smart grid-enabled proxy services.

The members of the SVPI have identified a number of key challenges that should be a priority in FP7. These include:

SVPI 1. Enrichment of semantic cooperative standards. There is a need for new enriched semantic-cooperative standards to define the security models and protocols (security context and personalised policies to observe within each such context as defined by the user) including those relevant to web services and smart proxy-enabled security context- sensing, context-sensitive accountabilities, security policy, model and protocol appropriation.

SVPI 2. Virtual communications domains. A new breed of communication management (including middleware) will be needed along with more expressive semantic-cooperative service description and session configuration resolution to hide the complexity of security-context-aware personalised privacy and security protection from both the user and the application layer. This is to support the ***modelling and inter-operation of*** virtual communications domains across whose boundaries scalable context- aware security and trust services could thus be invoked in a graceful, dynamic and seamless fashion. It is crucial to examine the pre-requisites to underpin the virtualisation and semantic architecting that is required to enable the graceful integration of various security technologies, including legacy, evolving or new technologies.

SVPI 3. Architectural Challenges. Whilst the virtualisation paradigm powerfully underpins the Open Metropolis and multi-layer security protection objectives, it, at once, implies and supports significant other architectural capabilities whose availability within each trust domain and security context would significantly add to resilience of the security protection; so ideally, we aim for additional virtualisation-enabled capabilities for efficient and effective:

- S&T threat scenario situation assessment
- S&T threat scenario pre-emption & threat chain breaking
- S&T threat scenario forecasting, simulation, socially intelligent fixes & failure recovery policies enactment
- S&T threat pre-emption eco-system (immuno-genetic modelling) to combat the attackers' eco-system i.e. match the attacker's re-learn-re-innovate-re-attack chain so as to enable enhanced pre-emption, prevention and recovery in a dynamic attack environment.

8.4.6 Internet Infrastructure Security Initiative (IISI)

IISI focuses on security models and technologies for GRID, advanced cryptography for multimedia Internet and e-commerce applications, secure software for the future Internet, novel trust and security models for Internet and interoperable ubiquitous computing environment, dependable home connectivity as the advent of ambient intelligence, privacy, authentication, accounting and reliability for Internet.

The members of the IISI have identified a number of key challenges that should be a priority in FP7. These include:

IISI 1. Novel trust and security models for the internet. The Internet technologies of the future will be charged with securing the Internet layer issues of content integrity and confidentiality. Research will largely focus on developing novel trust and security models for the Internet and for the interoperable ubiquitous computing environments that exist today and for those in the future.

Such security models would involve defining new mechanisms to provide confidentiality of Internet content, to provide secure authentication. There is also a requirement to obtain stronger and more reliable procedures of accounting and non repudiation of future Internet content handling, in particular with future e-commerce applications. Research here will focus more on advanced cryptography designed specifically for multimedia content and e-commerce applications.

IISI 2. Security and Reliability in home internet connectivity. New avenues of research will need to be undertaken to provide not just security but also reliability in home Internet connectivity with the advent of prominent intelligent ambient devices. Security network management of these future home Internet devices will be addresses to assure security and safety is utmost across devices with different security capabilities.

Due to the fact that so many objects of the future will become interconnected, researchers will need to direct their efforts to ensure that there is a protocol or standard in place to develop scaleable Internet security technologies across different platforms.

IISI 3. GRID Security. There are numerous complex challenges in making GRIDS secure and trustworthy. Some of the problems are serious challenging as they require a high level of abstraction across very different technologies and areas of competence.

IISI 4. Secure Code development. Secure code development will be vital to defend the Internet protocols from code exploits (buffer overruns and so forth). Both Internet code management and code risk analysis standards and methods will need to be developed to ensure that the code (largely FOSS based) is able to withstand new environmental threats. Secure Internet code management will incorporate new mathematical proof methods that will help verify and certify code is correct for its intended operation.

The future Internet security layer will provide many challenging research areas open to the European knowledgebase to solve in order to provide secure, reliable and always on ubiquitous Internet environment.

IISI 5. Decisions regarding existing SOA. The Internet layer will take existing state-of-of-the-art (SOA) Internet technologies and decide either to build upon and extend these standards or to develop completely new standards that better describe a new internet movement based on past and current experiences. Such components to be addressed are current secure and authentication protocols such as IPsec, SSL and so forth. Can current secure code development standards be extended or do we need to re-develop new standards? Research will also look at existing methods of code verification and how best to build upon those methods and standards.

8.4.7 Application Security Initiative (ASI)

This initiative is directed at improved and novel approaches to application level security measures. New architectures and end-to-end security design issues to protect at an application level in future networks. The following areas are being investigated: security tools, policies, context management, allowing trusted users to view documents, single sign-on, digitally signing web pages for example, application vulnerability validation, anti-virus and so forth.

The members of the ASI have identified a number of key challenges that should be a priority in FP7. These include:

ASI 1. Global Application Security Processes in the development of Application Level secure systems. In order to increase the security and dependability of the Application layer and to ensure application compliance and measurement quality, the developers must be properly trained and they must follow a global application security process, with phases that follow closely the application development phases from the idea/proposal/mandate phase through to the disposal phase. One of the major challenges is to develop scalable application level secure (AS) systems. Not only must the AS systems be scalable but they must be created in a way that provides a solid measurement of quality of service. In achieving these goals, proper code analysis must be undertaken that leads to secure code development in a standardised way. The end goal is to have a QoS security service that is scalable and is resistant to attacks in particular Malware and Spyware epidemics.

ASI 2. Application level security services in a distributed web enabled environment. (Interrelated to IPI, Biometrics, IISI, SVPI challenges) Applications running in pervasive and ambient intelligence environments must be capable of providing always-on mobile security and privacy. Significant research must be carried out to enable the applications to work with the new technologies being developed in the identity and privacy management areas, biometrics and internet infrastructures areas. For example, authentication and identity management systems in service-oriented architectures (SOA) built on Web services. Web services are essentially decoupled applications and the identity management is part of the underlying infrastructure. Therefore, in this domain, we are focused on dynamically responsive Security and Trust Chain service provisioning, which can hide the complexity of context-aware personalised privacy and security protection from both the user and the application layer. In order to accomplish this, there will need to be three virtual communication domains across whose boundaries scalable security services could be invoked to manage a user’s dynamic Security and Trust chain in the context of user’s business logic and value chain. Therefore, for each such client device/user, three interacting domains are virtualised to include all hardware and software modelled under each of:

1. Self-Domain (S): All HW/SW constituting user’s personal client devices: home computer, office computer, laptop, PDA, mobile phone and native applications running on them (calendar, diaries, profilers etc).

2. Others-Domain (O), All HW/SW belonging to all other parties transacting with the user including that of peers and grid-enabled services.

3. Smart-Middleware-Domain (M): Any component involved in mediating data exchange across the boundaries between the above two domains.

Thus, there are key research challenges arising from the need for graceful and reliable integration of the above virtualised environments within a secure, efficient, service-oriented, application centred, model-based, context-aware and event-driven computing environment.

ASI 3. Adapting traditional security frameworks to OSS development methods. Free and Open Source Solutions (FOSS) needs to be secured, but it needs a specific focus. Particularly in the public Sector, FOSS is considered a critical component providing a way to improve:

- Transparency
- Sovereignty
- Ease of experimentation
- Open Sharing of knowledge.

Security in Open Source used to be a minor concern for two very different reasons. On one side, most of the Open Source applications were not seen as "business critical". On the other side, Open Source Infrastructure applications (mail, web server, routing, DNS, ...) had been around long enough to be run under the gauntlet of various security attacks to be now quite secure. Moreover, with a development model that enables and encourages source code scrutiny, there is a general feeling that security issues are easier to spot and to solve by the community.

But with the wide adoption of Open Source solutions, the quantity of code to look at has grown significantly and the number of applications that are business critical has grown proportionally also. Moreover, new issues like Cross-Site Request Forgeries (CSRF) or (Cross-Site Scripting) XSS attacks are appearing at the application level. This leaves the FOSS world with issues of accountability and certification, and normalisation of architecture.

A major challenge will be adapting traditional Security Frameworks to the Open Source development methods. Trying to solve these using conventional processes will most probably not work, trying for instance to demonstrate that a specific firewall meets specific security requirements is not a trivial exercise. Therefore, the FOSS communities should adapt the process they already very successfully use to develop applications to also manage the security issues of their applications, and applications interactions/architectures. Much of the FOSS success is linked to the way FOSS infrastructures are built: what is commonly referred to as "FOSS relies on the collaboration of the Cathedral and the Bazaar to build a city".

We needs to build a framework where the security needs of an Architecture can be modelled, defined, reviewed in an open and transparent manner, using the same "Forges" the application development already use. Basically defining a "contract model" between application elements, thus enabling not only the collaboration of application developers within a comprehensive framework but also the collaboration of service providers on a live application.

The goal is obviously not just to guarantee that an architecture «can» be secure, but that the specific way this architecture is run is secure.

8.4.8 Methods Standards Certification Initiative (MScI)

The MSc Initiative of the Security Task Force is placed clearly within the existing European Commission policy on security with reference to

- Interoperability of security
- awareness building on existing security standards and their promotion
- the evolution of present security standards
- development of new security standards where appropriate
- Facilitating the existing security standards development process via
    - National Standards Bodies & International Standards Organisation
    - European actions through CEN/ISSS, CENELEC, ETSI

The members of the MScI have identified a number of key challenges that should be a priority in FP7. These include:

MScI 1. Response time of Standards development process (note from Chair: this should be addressed within the other initiatives and doesn't really belong in MScI)

It is interesting to note that the ISO SC37 WG6 is developing standards on cross jurisdictional and societal uses of biometrics.

Is the standards development process able to change and respond to the new changing paradigm on current challenges to the Security and dependability community, which can be summarised as:

- From perimeter protection to the holistic, integrated system security

- From central access controls to decentralized usage control
- From patch management on demand to long-term sustainable security
- From security as a product to security as a dynamic process.

MScI 2. Shorten time of Standards development process. Current security standards development is a long process covering from 2 to 5 years. There is a fast track approach, which takes from 6 months to 1 year. There is a real need to shorten the time it takes to develop a consensus on a standard within the ISO world. W3C, IETF, ITU, ISO etc. are all working on identity and integrating the concept of identity into certain standards. Liaisons between the different organisations are, mostly, in place. However, strong liaisons have not always been established with ISO SC37 Biometrics and this shows that the existing ways of working together are outmoded, outdated and take too long. For example, ISO takes at least 30 months to fast track acceptance of a standard. New ways of working must be found to bring the standards process into tomorrows world. IF NOT ADRESSED, this will continue to be extremely inefficient process.

MScI 3. More Community participation to standards bodies. There are currently very few participants from the user community, especially from SME sector (availability of English speaking personnel) and New Member States of the European union (cost factor and lack of resources of the national standards body).

Most existing participants come from universities or industry. The liaisons between the different standards organisations are not always clear cut, and even within ISO, there can arise divergence on who is responsible for what. Currently, there are three sub committees which are working on security SC37(biometrics), SC27 (security methodology & process) and SC17 (cards).

Amongst the European countries, there is only the UK that doesn't charge for participation in the standards body - BSI IST/44 biometrics for example. So this is a barrier stopping qualified professionals from participating in the International Standards organisation process. If not addressed, a real European contribution to the standards process will take far longer to build.

MScI 4. Security Certification major growth area. Certification in security of products, people and companies is a new field and a major growth area. For example, there is still no European test centre for biometric vendors, and most countries have yet to agree a certification centre for ISO17799 (security methodology) or ITIL (BS15000) (service management of IT systems).

The most important challenge in identity security is in the interoperability of biometric vendors products. The ISO19794-2 standard has just been published together with 3 others. Currently, no vendor can declare themselves conforming with this standard, there is no accreditation of European laboratories from the national bodies such as UKAS in the UK. The MIT project will begin in January 2006 and to some extent will move forward in this area. It is hoped to have certification of vendors at the end of 2006 but ID cards and passports are already being issued with non-interoperable biometric algorithms. Therefore, by 2007-2008, we should have the beginnings of an healthy European certification industry for interoperable biometric algorithms and sensor devices. BUT WHAT ABOUT THE REST OF THE SECURITY INDUSTRY ?

8.5 Mobile and Wireless and Smart Card Research Projections:

Note: It was decided that the Smart Card research should be included in the Terms of reference of the Mobile and Wireless Security Initiative (WSI).

8.5.1 Wireless Security Initiative (WSI)

This initiative targets security in Mobile/ Wireless service environments. It addresses Ambient Radio, Ambient Networks and User Device capabilities in a 3G/ beyond-3G, Ad-hoc and All IP networks. It addresses mobile, wireless and smart card technologies covering the development of new protocols, interfaces, technology interoperability and future standardisation issues in this space.

The members of the WSI have identified a number of key challenges that should be a priority in FP7. These include:

WSI 1. Convergence. The future is all about Convergence, which brings forth an environment with new requirements and challenges and evolving standards, which only define a part of this since any of the disruptive technologies come from industry fora. 35% of current Telco suppliers are IT companies. This percentage will increase in the future- it also means that security procedures defined in the Telco standards do not and will not apply in the future. The ″Rules″ are changing. So Policy known today need not apply tomorrow. How do we still maintain Privacy and the Telecom laws to avoid regulatory conflict.

WSI 2. Definition of Optimal security roadmap. It is clear there is a need to give Security the highest priority. However, can this lead to overly secure concepts? We need to find the right balance in defining the future so that FP 7 can offer enough of interesting mid- and long term topics for research and that Projects produce valuable results for the standards and Industry to commercialize on.

WSI 3. Integration of existing technologies. .A number of Security Solutions already exist. Most of these have been either deployed or are innovative proposals out of research and new industries. However, there is also a lot of repetition or very similar solutions yet leaving holes in between that haven't been addressed. The challenge here is, how do you harmonise these to avoid additional cost and performance loads deficiencies on the network. For example, how can carriers/operators efficiently make use of the solutions-eg, USIM/ISIM. The challenge is to map the transition steps towards the future?

Joint Security and Dependability and Mobile and Wireless Workshop

A Joint Workshop (JW) was held in May 2006 between the Security and Dependability Community and the Mobile and Wireless communities organized and hosted by the SecurIST project. These challenges were discussed and elaborated at this event. The following mindmap (Figure 10) depicts the topics taken for a number of streams in a cohesive and comprehensive manner[72]. In order to clarify the research priorities, they will be broken into three categories:

1. Mobile Software, Services & Information topics, which deal mainly with socio and technological aspects of software, services and exchange of information mechanisms.
2. Secure Technologies, Mechanisms & Virtualisation topics, which address security technologies, mechanisms, and architectures, and the challenges arising from them specific to mobility and wireless connections.
3. Mobile end user aspects, which deal with topics from the user's perspective – where the user is not only the end-user or 'customer' with the mobile terminal, but also the provider of services, the communications provider, the network operator and all the human hands involved in delivering and supporting the envisaged ambient environment.

8.5.2.1 Software, Services and Information Access

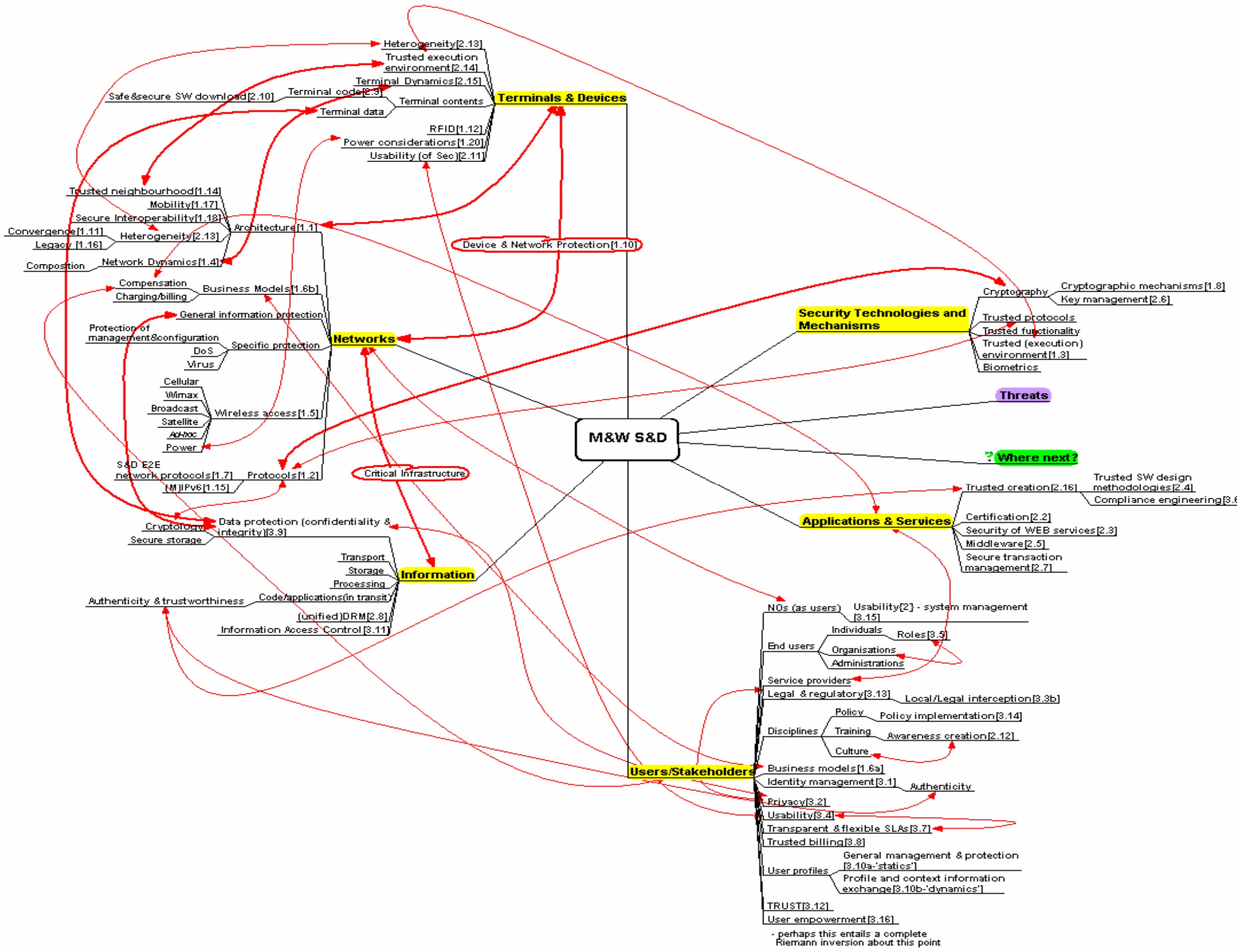
The emergence of open service-centric platforms, such as service oriented architectures (SOA) using web services, provides major opportunities to position the European software industry at the heart of the emerging information society. However, the uptake of solutions based on software and services by industry, especially in the mobile and wireless environments, are dependent on all stakeholders (industry and end users) confidence in their security, trust and dependability.

There are a number of both societal and technological challenges for the medium and long term research and development to enable security, trust and dependability in the areas of Mobile Software, Services and Information access. These include the following priorities.

JW1. Secure data management, and synchronization and private exchange of user profile and context information. One of the future challenges for FP7 is a paradigm shift of gradually replacing the physical boundaries with logical boundaries maintaining context in order to move from a system-centric, or "Central-Command-and-Control" to a Citizen-centric, or "Empowerment of the Citizen" Approach to security. This view advocates a shift from global identification (database silos) to a context-specific local recognition (persistent logical identity boundaries determined by context) and the elimination on the dependence of compliance management to focus on sustainable security through citizen empowerment (giving the citizen the power to control their data. Few ICT technologies have been designed with this kind of scenario in mind so a gradual process of revisiting basic technologies is required to ensure that the context sensitive empowerment of the citizen is supported. The transformation will be much more than a quick fix and will require a sustained effort on all R&D levels to ensure understandable, interoperable, secure, convenient and efficient systems.

JW 2. Efficient encryption and cryptographic mechanisms and algorithms suitable for different types of devices and networks. Cryptology research continues to deliver a stream of important results, but work must continue to keep abreast of trends in network volume and performance, and of the development of new attacks and insights into vulnerabilities. When we evolve to an ambient intelligent world, privacy concerns will increase and cryptology will need to be everywhere (even in the smallest devices). This means that cryptology will be needed that can offer acceptable security and performance at very low cost (hardware footprint, power consumption). Cryptology will be needed to distribute trust and to reduce the dependence on a single node. Challenges also include the need for very long term protection of sensitive or contractual records, and preparedness of the possibilities of quantum computing.

JW 3. Secure software and execution environment including O/S. The requirement may be divided into three levels: the trusted hardware to physically execute software; the trusted operating system that together with the trusted hardware provides the interfaces (APIs) available to operational software; the software itself which may be divided into two further classes (i) trusted, verifiable system software for, say, execution of cryptographic algorithms, secure protocols, and user interfaces, and (ii) trusted application software to deliver functional services. A further class of un-trusted software must also be provided for (sand-boxes etc.), whilst maintaining strict protection of the rest of the system.



D:\LocalCache\Projects\SecurIST\workshop\keyAreas\MM_02b.mmp - 31-05-2006

Figure 10 – Workshop issues and relationships

In addition to the design, implementation, and validation tools to deliver these, there is also the need for comprehensive modelling tools and environments to provide large scale simulation of design and of validation scenarios.

Research is necessary into more economical and practical ways of providing trusted components and systems. The delivery and deployment into real operational networks, services, and terminals also still need much investigation, prototyping, and assessment.

There are very serious issues here about how to preserve and utilise the current legacy of operational software with its multiple patches and its known deficiencies in terms of design and implementation rigor and the impossibility of full validation.

Other specific issues include: management and maintenance (e.g. upgrade) of certified software; the roles of the smart card in general and the SIM in particular; relationships to privacy and DRM; *trust* (q.v.), the need for automatic security evaluating tools during development process, and achieving truly high quality software - despite the large gap between best practice (and research) and industry average. Mobile service and OSS design must include up front security and privacy management, into service specification, instead of the current day approach as an "Add On". There is a need to enable the SW designers and security experts speak the same language for security specifications, or more specifically, have consistent and comparable expectations. There is a need for modelling security requirements: Analysis, Validation, etc. and a need for making SW applications dynamic ie. build context awareness into application.

JW 4. Identity management & privacy. One aspect of this topic concerns the mechanisms for user identification and authentication, and the means to protect users' credentials and sensitive information from unauthorised disclosure or manipulation; this is covered by **JW2** and **JW3**. The other aspect is the user expectation for privacy: the right to remain anonymous or unidentifiable in appropriate circumstances, and the ability to retain control, or at least influence, over the handling of personal or sensitive information released in confidence to other parties. There are two parts to this second aspect: the technical issues, potentially within the scope of **JW2** and **JW3**, again; the other part concerns the sociological and political issues arising, not least the ongoing tension between the legitimate rights and wishes of the individual, and the needs of society in its responsibilities to protect and benefit its members as a whole.

Two specific concerns arising in this area are: the need for legal interception in pursuit of law-enforcement, and with it the unease about abuse of the technical capability both by the authorities and by the unauthorised criminal; the second concern relates to the ability to build quite intimate personal models or profiles from apparently innocent scraps of information with a view to circumventing inadequate privacy protection – technical or procedural. A further topic that should referenced here concerns the current distrust by the subject – arising from an apparent over-confidence or reliance by the authorities – in the true effectiveness of bio-technology as the basis for identification. Its usefulness as a *component* of an overall identification scheme – or schemes – is welcomed. The main questions relate to vulnerability to identity theft and masquerade, as well as the basic fallibility of some current proposals.

JW 5. Secure and dependable end-to-end network protocols and applications enabling a simple-to-use trusted transaction environment. Research and business experimentation into managed security and privacy services, in mobile space, to create incentives turning burden/costs into opportunities is needed. It should be context aware and with dynamic reconfigurability/control so that the trusted environments and the hostile/volatile environments can be distinguished and be dealt with accordingly. Other challenges for e-2-e Security with mobility include secure neighbour discovery, MIPv6 and AAA integration, interdomain issues, and Key management. Security in sensor networks and rule based support of pervasive use of private protection.

JW 6. Unified Digital Rights Management environment. There is a need for an EU-based approach for digital rights management to enable the EU to become a more effective content creation and provision environment. In order to accomplish this to the benefit all of the stakeholders involved, it will be necessary to provide an framework and environment with protocols that will enable the traceability of the rights all the way back to the contents rights owner. There needs to be a proper balance between the rights of the producer, those of the supplier and the purchaser/user. Some of the technical approaches include included ontologies, asset identification, perceptual hashing and semantic linkages for traceability. These would have to cope with content that is changed throughout the whole chain ("who owns what and when") and the ability to observe the adherence to agreed rights. Best efforts must be made to enable transparency in rights distribution, and/or creation of DRM distribution networks. Addressing these challenges within FP7 could open up very new and exciting opportunities for special actors within this high growth potential area.

JW 7. Transparent and flexible Service Level Agreements. One of the long term challenges is to replace the current (unjustifiably trusted) system creation environment with an end-user based environment, which elicits their trust in a more proactive manner. This should be based on negotiation (or enforceable and sanctionable SLAs) between the end user and the provider in order to match the end user needs and their tolerable risk assessment criteria levels. This is considered a long term challenge because it cannot be done without revisiting, harmonising, changing and/or replacing the various approaches in use today. Currently, there is a lack of trust metrics to establish/define quality of trust and a well defined Standardised Trust Management model is needed with quantifiable metrics models for Security and Trust.

JW 8. Combined multi-layered mobility support and authentication/authorization across diverse networks and support of simultaneous use of multiple access technologies. Security for mobile services, which is independent of underlying access networks, will require seamless handovers requiring negotiations of new SLA. Virtualisation Interoperability standards are needed and heterogeneity requires flexible solutions and this flexibility opens holes in the systems and the attackers easily find the weakest links.

JW 9. Device and network protection against attacks (virus, Trojan, DoS, Phishing) and intrusion detection. Threats and vulnerabilities have to be identified and should be addressed based on level of security needed and user/application profile in an auto configuration mode, so that users get more trust in the network and applications. Such functionality will raise the trust among the users.

JW 10. Safe and secure software download enabling networks and device re-configurability. Dependability issues in safe/secure downloads must be addressed. Some of the issues include intelligent function firewalls, intelligent access controls, need for user friendly download and building up of software trust and risk awareness. There is a need for dependencies and security maps to provide traceability and to keep the users informed of what is happening and automatic reporting mechanisms should be in place.

JW 11. Mobile connectivity/integration to the GRID community. Another area of significant interest raised at the Joint Mobile and Wireless Security and dependability workshop was the future interrelationships and interactions between the mobile and wireless and the Grid communities. Security of today’s large scale, open, distributed heterogeneous systems (such as computational grids, peer-to-peer systems, pervasive/ubiquitous computing, etc.) has become a mainstream operational concern. Establishment of in-depth security services and trust relationships are the most desirable features for such systems. In a Grid environment, where identities are organized in VOs that transcend normal organizational boundaries, security threats are not easily divided by such boundaries. Identities may act as members of the same VO at one moment and as members of different VOs the next, depending on the tasks they perform at a given time. Thus, while the security threats to OGSA fall into the usual categories (snooping, man-in-the-middle, intrusion, denial of service, theft of service, viruses and Trojan horses, etc.) the malicious entity could be anyone. An additional risk is introduced, when multiple VOs share a virtualized resource (such as a server or storage system) where each of participating VOs may not trust each other and therefore, may not be able to validate the usage and integrity of the shared resource. Security solutions that focus on establishing a perimeter to protect a trusted inside from an untrusted outside (e.g., firewalls, VPNs) are of only limited utility in a Grid environment[74]. Conventional Grid Paradigm constitutes of secure dynamic virtual organizations relying on rather reliable networks accessible without any preconditions where users and resources are tight to a given location and network address. The context of a member of such a kind of collaboration is considered to be static and more or less equal to the one of all other collaborators. Context information such as device capabilities or available bandwidth is not considered. Next generation of Grid will have to allow its participants to be mobile. This includes nomadicity, change of network services provider during a session, support for device or session mobility, etc. Mobile Grid will offer a number of features to its users; however, its security design will become more complex as it will inherit all the security vulnerabilities of the mobile world. The security designers need to keep in their minds the intrinsic nature of both Grid (large scale distributed computing) and mobile worlds to come up with some adequate solutions.

8.5.2.2 Secure Technologies, Mechanisms & Virtualisation

The large R&D challenges arise from the increasing size and capacity, and, hence, complexity, of a global information system. The expectation is going to be for best possible connection for the delivery of ambient intelligence – connection anytime, anywhere, to any person, service or device. The anticipated expansion of size and scope brings with them a de-perimeterisation, with boundaries between networks and domains blurring and disappearing. This, in turn, leads to de-centralisation of control and a consequent shift of responsibility towards the user and service provider that raises new security and dependability challenges.

Research priorities include the overall architectures at both the conceptual or *virtual* level, for high level design, modelling, and policy making, and at the *real* level concerning the working, functional entities and interfaces, and the communications between them. The requirements are for seamless roaming and interoperability in a dynamically shifting environment composed of a heterogeneous set of entities and services. At the network level, dynamic overlays – again dynamic – will deliver a wide spectrum of user needs.

Added to this requirements-perspective, there is still the need for commercial viability and the support for many possible business models and relationships. The essential concept of trust, fundamental to network connections, requires solid foundations for both the subjective, reputation-related, aspect and for the formal, possibly provable aspect of the *trusted* device or entity.

To support all of this, there is the ongoing need for development of underlying engineering and research into new technologies to deliver higher security – but with increased performance, and at lower cost. These then need to be built into the protective mechanisms and countermeasures that can resist new forms of malicious attack as well as delivering the expected dependability in the increasingly complex environment with its even faster increase of possibilities for malfunction and mis-operation. Protection of the system operation and services must also cover attack-resistance and fault-tolerance.

The top priority items for the short, medium, and long terms were, respectively: for the trusted execution environment; for security to be independent of precise context (or, rather, to be optimised for the specific); and for complete architectural virtualisation. More details of the top priorities include[72]:-

JW 12. Meta security policies for independence of networks. The goal here is to create a generalised framework for specification of security policy that provides for specific application and interpretation at real implementation levels irrespective of local technologies, so as to create coherence and consistency within a domain. It also allows for creation of co-operating policies between domains.

JW 13. Virtualisation at architecture level. Research fundamentals include the overall architectures at both the conceptual or virtual level, for high level design, modelling, and policy making, and at the real level concerning the working, functional entities and interfaces, and the communications between them. The requirements are for seamless roaming and interoperability in a dynamically shifting environment composed of a heterogeneous set of entities and services. At the network level, overlays – again dynamic – will deliver a wide spectrum of user needs. The challenge is to identify a sufficiently general set of architectural components or building blocks and to specify their functionality, interfaces and the protocols that govern their intercommunication and interoperation. Ideally, we should aim for additional virtualisation-enabled capabilities for efficient and effective:

- threat scenario situation assessment
- threat scenario pre-emption & threat chain breaking

- threat scenario forecasting, simulation, socially intelligent fixes & failure recovery policies enactment
- self-x properties:
  - self configuration.
  - self organisation
  - self protection,
  - self defence,
  - self "healing",
- threat pre-emption eco-system (immuno-genetic modelling) to combat the attackers' eco-system i.e. match the attacker's re-learn-re-innovate-re-attack chain so as to enable enhanced pre-emption, prevention and recovery in a dynamic attack environment.

JW 14. Seamless interoperability. The appearance of seamless inter-operability could be achieved through a very large set of carefully specified bilateral agreements between communicating entities, or as a result of an architectural approach that results in sets of standard specifications for entities and their inter-relationships. This could then become a by-product or development of virtualisation at architecture level, as described above.

JW 15. Attack Resistance. Although this should be an aspect of many of the other challenge-items, it is important enough of itself to be separately identified. In addition to the development of counters to known, classic attacks, new attacks and vulnerabilities resulting from the expansion of the networks will be inevitable. Pre-emptive analysis can prevent some potential attacks through specific defences or avoidance. Defence against others may be possible as a result of the development of generic defensive approaches and strategies – ubiquity and redundancy. As back up to deployment of counters to attacks, there needs also to be parallel development of resilience strategies that provide for successful, rapid recovery following disaster, whether this be as a result of attack, malfunction, defective design or implementation, or just plain fat-finger problems.

JW 16. Radio Access Network, Core Network and Service architecture. There are also security and dependability requirements for Software Defined radio (SDR) including issues involving spectrum optimisation, the need for flexible services, certification of SDR platforms, local regulation on cryptography use, standardisation of SDR services and protocols, which are highly challenging because one has to balance the 'openness' and the 'controls'.

JW 17. Cryptology. In order to protect information stored or transmitted outside of a 'home' trusted environment, and even to provide certain trustworthy interfaces within that trusted home, specific challenges for cryptology research include[73]:

- *Crypto-everywhere*: software, hardware, and nano-scale implementations will be required as cryptography is deployed as a standard component of all communication and computation layers and – with ambient intelligence (or pervasive computing) – at "every" physical location. Requirements will be for lower cost, higher performance, specific applications, smaller size, low complexity, provable correctness, and low energy consumption.
- *Long-term security*: Many crypto-systems considered robust have been broken after a certain amount of time (between 10-20% years). For instance, most of the hash functions developed before 1993 have been broken. We need to build crypto-system that offer long term security, for example for protecting financial and medical information (medical information such as our DNA may be sensitive information with impact on our children, our grandchildren and beyond). In the medium term, we need to be prepared for the eventuality that large quantum computers could be built: this would

require an upgrade of most symmetric cryptographic algorithms and a completely new generation of public-key algorithms.

- *Provable security*: cryptography has been very successful in developing security models and security proofs within these models based on a limited set of assumptions but more work is needed to expand this approach to more areas in cryptology; automated tools to assist in developing and checking such proofs seem a promising research direction.
- *Secure implementation*: even if we are able to get theoretically sound cryptographic algorithms and protocols, most of their failures can be found at the implementation level. A design methodology and technical solutions to increase resistance to side channel attacks (power, radiation, timing attacks) and work on secure APIs would be very relevant.
- *Digital rights management*: several techniques such as fingerprinting and watermarking are available and there is a growing interest in this area. However, there is a lack of solid scientific basis (even just openness about techniques used in commercial products) and insufficient academic research.
- *Privacy*: diffusion of sensing, location based services, explosive growth of storage capacity and communication mechanisms, and data mining technologies present a major risk to privacy. The problem lies in the asymmetry of technology: advances in technology make privacy violations much easier, while protecting privacy is complex and delicate (integrated solutions are necessary that work at all layers – physical, network, transport, application). Ease of use plays an important role here too. Advanced cryptographic protocols can bring substantial advances in this area.

8.5.2.3 Mobile End User Perspective

Three of the principal end user-based concerns identified have many points of contact and overlaps: **identity**, **privacy**, and **user empowerment**. The common theme relates to users' requirements for appropriate control and visibility in matters that concern their personal, or their organisations', assets and sensitivities. This covers all aspects of information and communications services: from the simple voice call; to the complex high-value multi-party transaction; to profiles held by administrations or commercial enterprises. With all these, there is the enormous challenge of how to achieve the proper balance between the rights of the individual and the needs of society. The problems are generic in a converging ICT world, but the difficulties are considerably greater in the heterogeneous, dynamic mobile and wireless environment with respect to providing technical solutions, management of the deployed technology, and the inclusion or the user and user preferences in the loop.

The other large area requiring further research is user-based *trust*: how relationships between users and services, and between users and other users may be established, monitored, and maintained. Accompanying this, is the general requirement for trustworthy services – from banking to health to environmental monitoring – and with it the need for the underlying security technologies to keep pace, delivering higher assurance and performance with lower cost and size.

Further research and development is indicated for the many technical issues, together with appropriate complementary work in the human sciences: sociology and psychology. The following areas should be addressed in medium and long term R&D.

JW 18. User empowerment. This was a major topic of interest at the **"**Trust in the Net**"** Conference held in Vienna on 9th February 2006 [75], and has been reiterated constantly within the STF and Advisory Board (see Section 2.4, above - specifically Recommendation 1, and

Section 8.4.3 - specifically **SRI6** – *citizen* empowerment). The need for user involvement on security and dependability arises from two distinct sources.
The *first* is the user expectation of having appropriate control over personal or sensitive matters. Here the question is how to assign appropriate controls to the individual, as opposed to all controls being centralised in either major providers of choice – banks, Service Providers, etc.(discretionary), or monopolies – .gov, NHS, etc. where there is no choice.(mandatory); The issue is the general need for the user to be in control of its own information and resources, or rather the fear of not being in control: that, without the user's awareness, let alone permission, commercial, governmental, or criminal agencies may gain unauthorised control or knowledge of the user, possibly by aggregating seemingly harmless fragments (see **JW4**, above).
The *second* is as a consequence of the deperimeterisation that arises from the evolution of dynamic network architectures: appropriate controls will need to be vested in the individual, while some must remain the responsibility of certain service providers, and others, relating to physical aspects and operations, must necessarily be retained by the operators of the communications networks or their agents.

JW 19. Usability, Security, Trust and Dependability. There is a group of concerns relating to the usability, security, trust and dependability of applications and services accessible by the mobile user, together with those same aspects - usability, security, trust and dependability - of the actual communications media and channels. One may also include in this group the security-related services, functions, and interfaces, and the security of the mobile device itself. This obviously relates to the user *trust* aspects, below in JW21, as does the necessity of security and dependability in provision of any sort of trusted service. More elaborate scenarios envisage a dynamic, heterogeneous environment delivering ambient communications and services – seamless, secure, and dependable. Meanwhile how can the same ambience be exploited to contribute to the wellbeing of the planet and its occupants. Note: fundamental to the provision of trusted emergency services is the provision of dependable access; this is currently not delivered by most cordless DECT phone systems, which are dependent on mains power for operation, unlike old-fashioned PSTN connections and the mobile phone.

JW 20. Trusted device. There is a requirement and expectation about exploiting and extending the capabilities of the mobile device to make aspects of our lives easier and more easily managed: as a generalised access control device to enable physical access, and to provide login, signature, etc.; as a universal payment token, electronic purse, and authorisation tool for higher-value transactions; and to provide storage of and access to information – local caches and secure vaults: instant facts and figures as well as critical personal and health-related data. All of this is dependent on the trustworthiness of the device itself, and of the services accessed.

JW 21. User Trust Aspects. Two aspect of trust are identified: subjective – dependent on personal feeling or belief, supported by, say, reputation systems and frameworks; objective – based on assurances of verifiable trustworthiness of hardware or software functionality, including cryptography, trusted computing, security protocols, etc. Some form of metrics are required on which trust-based decisions may be made. Questions arise about how trust is established, maintained, monitored and reported, and how charging and payment can be made trustworthy. Considerable technology is already available; however, accompanying work is required to provide human sciences/ engineering support. The challenge is to establish a comprehensive framework for handling trusted relationships between all relevant entities, not just human users. Further investigation is required into the possible role of trusted parties as referees or brokers: how are credentials established? What are the liabilities of an entity that charges for trust-related services?

JW 22. Usability. From the naïve end-user to the expert system manager, the issue of usability of security is of great importance. The provision of all sorts of procedures and technical measures is valueless if they are not to be correctly exercised, either through ignorance or wilfulness – or even necessity, if the design is actually wrong.

In addition to the provision of the necessary technical interfaces, research is indicated into the design of the human interfaces and procedures, and the design and provision of contextual help and support, as well as preparatory instruction and training.

The research challenge is what can users actually understand: of the interfaces and available instruction, and also of what is actually going on, and why – in particular, are critical situations recognisable to the combination of the system manager and his toolkit?

JW 23. Regulatory issues and legislation implications. The need for significant research into the relevant legal and ethical issues is required for mobile computing (especially ambient intelligence, pervasive computing), an arena that is facing a serious resistance because of these issues. With the general trend of outsourcing services to external companies/countries, we need to evaluate the 'impacts of outsourcing of security functionalities' also relative to the legal framework in which the outsourcing takes place. Outsourcing is creating a new business relationship that "intervenes" with an existing one, and, thus, the issues of data protections laws are in danger of being forgotten. They are very important and, therefore, the challenge is multidimensional and not only a technological one. Moreover, policy makers need to be exposed within actual projects to economic and social risks of R&D security.

Some of regulatory and legal challenges include the (i) creation of new, or the modification of existing, laws and/or regulations or (ii) identification of a new legal and regulatory body to enable sanctions and enforcement abilities for security and dependability, preferably outside of the government sphere. There is also a need for the research and business experimentation, including real users involvement and input, to be carried out and tested in the funded projects. There is a need for truly interdisciplinary FP7 RTD projects related (not just) to usability - societal and business driven, as opposed to just technical – that typically need to be of long duration; because interdisciplinary research takes quite a while to become effective as the people from different disciplines learn to work together effectively.

JW 24. Effective and effective Certification Environment. The elements required for an effective and economic certification environment would require an evolution of security metrics to determine the levels of security. Today, security services are either enabled or disabled and finer granularity is required. There is a need to increase certification level transparency. i.e. relate security increase to level increase and risk decrease --> economic impact of certification. Cross certification amongst different service providers e.g. via real time negotiation algorithm and dynamic certification with virtualisation for third parties based on trusted community is needed.

JW 25. Future Business Models. There is a need to look at the quantified business impact of having security and dependability, highlighting the associated economic losses, so as to wake up people without unnecessarily frightening and/or discouraging them. Security should be a business enabler and not a showstopper and we should be capable of correlating security impact with business impact in real time with advanced security analysis tools.

8.6 Biometric Research Projections

8.6.1 Biometric Security Initiative (BSI)

The Biometric Security Initiative (BSI) is concerned with new algorithms, alternative solutions, novel pattern recognition approaches, multi-modal biometrics, data fusion issues, standardization of testing bio data and so forth. The initiative focusses on the elements dealing with the integration of biometrics in ICT systems, enabling new technology development in basic biometric technologies to leverage trust, confidence and security, across biometric authentication chain and identifying key features to put the technology to work and to meet requirements of real world applications.

The following challenges were identified by the members of the BSI as their key challenges for FP7.

BSI 1. European leadership in biometric development across the authentication chain. Europe has proven expertise in building reliable biometric systems this is rare in the current environment, there are already mature systems working in Europe. We should support the development of mature, secure and dependable systems and avoid the deployment of immature systems. Those early systems are not technically correct and propagate a negative perspective on biometrics systems.

Europe demands the establishment of a European test and certification centre, in order to support European organisations (government, companies and users) in making appropriate decisions and adopting the right technology. In the short term, current FP6 projects are investigating novel biometrics and integration is taking place, three novel pilots covering wide range of applications and future use of biometrics. In the medium (2007-2010) and longer term (2010-2013), further exploitation of physiological biometrics will need to be researched including the use of even less obtrusive sensors.

BSI 2. Promote European values in the integration of identity in the network society paradigm, taking into account the European cultural space. Harmonisation of Biometrics across Europe. A network society calls for continuous integration of applications in new areas (eGovernment, eHealth, etc…). Those applications are not probably new outside the European geographical space, but Europe should integrate them in a respectful framework. It will lead Europe towards the excellence and the reference in the deployment of network services.

An important step towards this challenge is the scenario development, where pilot systems are designed, integrated, built and studied in a controlled, adaptive and evolving environment, with the opportunity to become “research testbeds” for the adoption of biometrics in every day scenarios (private spaces, electronic signature, network applications). This would enable the gathering of real data on the impact of the deployment of biometrics at the socio-economical level.

Another important feature of the deployment of biometrics is embedding data protection into technology deployments and architectures through development of specifications, protocols and tools to keep the required level of assurance and certification. By means of new tools, organizations and users may evaluate the compliance of systems towards legal, security and dependability risks and conformance.

In the short term, in current FP6 projects, the BIOSEC biometrics API are bring used, standardization, contribution to the relevant biometrics standards are being undertaken and three novel pilots covering wide range of applications and future use of biometrics. In the medium (2007-2010) and longer term (2010-2013), there is a need to address the creation of new standards and modification of the existing ones in order to cover the use of new biometrics modalities that will result from IST project HUMABIO R&D, including standardization of authentication procedures/protocols.

BSI 3. Leading Europe towards developing cutting-edge technology. This would include novel pattern recognition approaches that would support the integration of biometrics in the ICT systems of the future. In addition, testing procedures and tools, towards security certification and/or evaluation of biometrics systems (databases, testing protocols and procedures, compliance tools).

Multimodal biometrics is the key for massive deployments of biometrics, but several issues are in the agenda of researchers: testing and supporting tools, efficient algorithms, guide to choose suitable combination of biometrics according to applications, etc.

Europe is already leading the research in Aliveness detection, but an important support is required to keep the path. Those features will support the development of identity providers in the network society.

In the short term, EEG, ECG, ERP biometrics will be studied and utilized in working prototypes for the first time. Use of novel unobtrusive sensors for physiological measurements applied in biometrics for the first time. Work will be carried out on token based systems (ePass, ECC), biometric template protection (compact coding), robustness against system noise to allow hashing and application in 1-to-1 comparison scenarios. In the medium (2007-2010) and longer term (2010-2013), further miniaturization of the biometrics sensors, complete unobtrusiveness for the subject, integration of the biometrics system with the ambient intelligence infrastructure, transparent and continuous operation of the system will need to be addressed. Future work will need to be done on DB based systems (Visa information systems, industrial environments), renewability and revocability of stored templates, application in 1-to-n comparison scenarios, automated self-identification, ICAO's perspective: unattended border crossing, exploitation of the three-dimensional acquisition space and proof fake resistance.

9 Annex IV – Relationship of STF Challenges to Advisory Board recommendations

This Annex maps the research challenges identified by the EU Security and Dependability Task Force (see Annex III) to the Advisory Board's recommendations in both the medium (2007 – 2013) and long term (2010 – 2013). This approach will enable the formation of relevant project consortia in a comprehensive and cohesive fashion ensuring there are no gaps in the required areas of coverage in the medium and long term.

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
CRI 1.	**Cryptology in an ambient intelligent world.** As we evolve towards an ambient intelligent world, and privacy concerns will increase, cryptology will need to be available everywhere – even in the smallest devices. In this context, cryptology will be needed that can offer acceptable security and performance at very low cost (hardware footprint, power consumption). The importance of "distributed trust" (or secure multi-party computation) will grow in order to reduce dependency on any single node – "you can trust this because you don't have to".	5. Development processes 7. User centric standardisation 9. Technologies for security	1. Empowerment, 3. Availability 9. Technologies for security
CRI 2	**High Performance algorithm for authenticated encryption.** High performance algorithms for authenticated encryption will be needed to deal with communication speeds and storage size that are both growing faster than the speed of processors. Some of the storage applications need cryptographic techniques that offer long-term security for long highly sensitive data (50-100 years). This also includes the developments of new algorithms that offer stronger resistance against mathematical advances and even quantum computers.	5. Development processes 9. Technologies for security	3. Availability 5. Development processes 9. Technologies for security
CRI 3.	**Advanced crypto techniques for media protection.** This challenges includes Advanced crypto techniques for media protection (authentication, copy protection/detection, perceptual hashing, Zero Knowledge watermarking and fingerprinting).	5. Development processes 9. Technologies for security	3. Availability 5. Development processes 6. Preservation 9. Technologies for security
DAMI 1.	**Development of secure and robust watermarking algorithms..** Digital watermarking, i.e. the possibility of imperceptibly and indissolubly attaching a piece of information to a hosting digital asset such as a video, a still image or an audio file, has been proposed as a viable solution to several security problems related to the way digital assets are handled in our digital age. The addressed problems include ownership verification, copyright protection, tracing of illegal uses and/or non-allowed redistribution etc. The initial enthusiasm about watermarking technology froze soon when researchers realized that the security and robustness requirements set by practical applications were very difficult to fulfil. Yet, digital watermarking remains one of the few solutions (in some cases the only solution) advanced so far to enforce digital rights managements legislations in highly non-structured scenarios. The main challenge researchers are still facing regards the development of a watermarking system that is robust against the several manipulations digital assets may undergo during their life cycle, and secure against any explicit attack against it brought by a malevolent third party usually termed pirate or attacker. In the last few years important advances have been made towards the definition of a general theory of watermarking robustness and security that can be used: a) to set the ultimate limits of watermarking technology; b) to rigorously measure the security of a watermarking system; c) to compare different systems from a security perspective. Yet, the development of a watermarking scheme that is at the same time secure and robust is still an open issue, possible the most crucial one, for which an answer will have to be searched in the next few years.	5. Development processes 9. Technologies for security	3. Availability, 4. Interoperability 5. Development processes, 9. Technologies for security
DAMI 2.	**Asset authentication through intrusive (watermarking) and non intrusive (digital forensics) techniques.**	5. Development	3. Availability

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	Authentication of digital data has been traditionally addressed by means of cryptographic primitives, such as digital signatures and hashing. Such techniques, though, guarantee the perfect integrity of electronic documents since authentication fails if even a single bit is altered. Such a strict definition of authenticity is not always appropriate for multimedia data where there is an interest in permitting some alterations that retain the perceptual meaning of the original content. Furthermore, when a prohibited alteration is made, it is desirable to not only detect that a change has occurred, but to also identify where in the document the change is, and possibly to have at least an idea of which the original content was. The techniques proposed so far to deal with asset authentication can be split into two fundamental groups: invasive and non invasive techniques. According to the former approach, authentication is achieved by first inserting within the to-be-protected asset a digital watermark whose presence and integrity is later on taken as evidence of authenticity; the latter approach belongs to the wider class of digital forensics techniques, and tries to acquire authenticity evidence a posteriori, without altering or damaging the original, for example by relying on the intrinsic and singular noisiness of acquisition devices (e.g. the ccd array of digital cameras). In both cases the development of advanced techniques permitting to discriminate between allowed and non-allowed manipulations, e.g. between manipulations that does not alter the semantic content of the to-be-authenticated document and does altering it, is an active research topic for which efficient solutions will have to be found in the years to come. Authentication security will have to be addressed as well.	processes 9. Technologies for security	4. Interoperability 5. Development processes 6. Preservation 9. Technologies for security
DAMI 3.	**Asset identification: perceptual hashing.** An essential ingredient in any secure multimedia application is unambiguous document identification. Besides the techniques that are known from computer science, that being bit-wise precise do not fit the nature of multimedia assets, two main approaches are currently being put forward being more focussed on signal processing and perceptual aspects. The best known of these methods is digital watermarking and is addressed by challenge 56. The second method is known under a set of different names such a perceptual hashing and perceptual fingerprinting. This method is characterised by the extraction of perceptually robust features (in analogy with human fingerprints) that uniquely characterise the content of the to-be-identified document. Despite the good opportunities offered by the perceptual hashing approach to identification, two fundamental questions have to be answered before perceptual hashing can be effectively used in practical applications: Which are the perceptual features that could better serve the purpose of data identification? What is the sensitivity of the human senses with respect to such features? This simple formulation hides very difficult problems due to the fact that perception is a very complex process involving sensory mechanisms of different levels. Other hot challenges in this field regards: a) the derivation of theoretical bounds on fingerprint size; b) the relation between fingerprint and quality; c) the benchmarking and comparison of different identification systems.	5. Development processes 9. Technologies for security	3. Availability 4. Interoperability 5. Development processes 6. Preservation 9. Technologies for security
DAMI 4.	**Conditional access to the digital assets.** Another essential ingredient of any secure asset management system is the possibility of restricting the access to the digital assets, or part of them, to authorized users. Whereas cryptographic techniques are an obvious solution, the interplay of encryption and signal processing must be carefully considered. In order to allow a secure, fast, and flexible access to the digital assets, it is in fact fundamental that the cryptographic primitives are adapted to, or, even better, jointly designed with the asset format. This is the case, for example, of secure access to coded data, e.g. a compressed video or audio file. Being the encryption of the whole bit stream unfeasible for complexity reasons, it is necessary that only some critical parts of the stream are encrypted, without loosing security or coding efficiency. At the same time it may be desirable that the partial encryption of the bit stream does not prevent a	1. Empowerment 5. Development processes 9. Technologies for security	1. Empowerment 3. Availability, 4. Interoperability 5. Development processes 6. Preservation 9. Technologies for security

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	flexible access to the coded data, e.g. it should allow fast forward and backward playing modes and fast searching. Finally, different users may be allowed to access different parts or different quality levels of the digital assets according to their rights, thus calling for multi-level encryption. Reaching all the above goals simultaneously is a very complex task that is better addressed if coding and encryption are performed jointly.		
DAMI 5	**Asset processing in the encrypted domain.** Most of the currently available technological solutions for "secure manipulation of signals" simply try to apply cryptographic primitives in order to build a secure layer on top of the signal processing modules, able to protect them from leakage of critical information. When cryptography is used as a module operating separately from the signal processing part of the application, we typically have to assume that the involved parties or devices trust each other, and that the cryptography layer is used only to protect the data against third parties not authorized to access the data or to provide authenticity. In many cases, though, this is not the case, since the owner of the data may not trust the processing devices, or those actors that are required to manipulate them. This may result in a lack of security of the overall system. It is clear that the availability of signal processing algorithms that work directly on encrypted data would be an invaluable help for application scenarios where "valuable" signals must be produced, processed or exchanged in digital format. Whereas the development of tools capable of processing an encrypted signal may seem a formidable task, some recent, still scattered, studies, spanning from digital watermarking, through secure compression, and access to encrypted databases, have shown that the application of signal processing in the encrypted domain is indeed feasible. Though promising, these studies are of an embryonic nature, hence many open questions about the potentiality and limits offered by the application of signal processing tools operating securely on encrypted data need to be addressed. While it is immediate to recognize the difficulty of the problems on the ground, it is easily understood that their, even partial, accomplishment would lead to the foundation of a new interdisciplinary research field, with a profound impact on the way we process, store and communicate multimedia data.	1. Empowerment 5. Development processes 9. Technologies for security	1. Empowerment 3. Availability 4. Interoperability 5. Development processes 6. Preservation 9. Technologies for security
DAMI 6	**Covert Communications (steganography and steganalysis). requirements formulated by law enforcement.** Another key issue is the possibility of establishing a covert communication channel by means of steganographic tools. Whereas one may wonder about the legitimacy of this action, it is clear that the existence of a covert channel between two parties wishing to communicate would be of great help to protect the privacy of the communication and the anonymity of the participants. On one side this can be a desirable feature in our age where any of our actions may be easily monitored without our explicit permission. On the other side, it may be the case that the covert channel is used for malicious purposes, e.g. terrorist activity. For this reason, reliable and accurate detection of covert communication could prove vital in the future as the society creates defence mechanisms against criminal and terrorist activities. Fast and reliable identification of stego media objects and estimation of the secret message size and its decoding are among the highest ranking requirements formulated by law enforcement.	5. Development processes 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 9. Technologies for security
IPI 1.	**Potential unforeseen risks with the unauthorized or unintended use of computerized personal identity information will increase.** One of the major challenges in collecting personal data at various points of contact is how to be sure that the data is treated according to the requested security and privacy standards and how anyone can assure that the data is only used for the intended purpose. In that respect, key issues in the future will not only comprise how to treat individual data that have been collected and processed for a specific purpose, but also include how combining of data on an individual to derive an own profile can be managed. Such a profile may make the "traditional" ID concept obsolete. It remains to be seen how profiled individuals will respond if this data set is false or if it is misused.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 7. User centric standardisation

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	New technologies or services may also lead to new risks to privacy: In many cases additional data is processed - sometimes only because of a naïve implementation without the real need for those data. Often the processes are performed seamlessly which may be good for convenience of use, but also means that most users are not fully aware about what is exactly happening and whether and how their private sphere is affected. Examples are location-based services or systems in the field of ambient intelligence which may release and transfer personal data without knowledge - and, hence, without consent - of the individual.	security	6. Preservation 9. Technologies for security
IPI 2	**Qualification of numerous new identification methods and new identity management systems.** Another key challenge will be on how to qualify new identification methods and new identity management systems for providing secure, reliable and privacy-enhancing ways to process personal data. The compatibility of these systems across technologies and across different countries will also have to be evaluated. Especially in the field of biometrics it is not fully clear which side effects may occur, e.g., what medical data could be extracted from the biometric raw data of the individual or accordingly the biometric templates. As part of a first comparison of different identity management systems, deficiencies have been found concerning the privacy and security functionalities of these systems which are also typical for other ICTs. For example: The standard configuration rarely addresses privacy functionalities sufficiently. Furthermore, people are not or at least not enough encouraged to utilize their privacy rights such as access, correction of data, deletion, withdrawal of consent etc. Technology could better support such privacy control functionality. Many technical systems dealing with personal data do not generate digital evidence which can be used to enforce a right and which is also accepted before court. Additionally, many of the systems today do not have sufficient protection mechanisms in place to prevent identity theft. All this applies to ICT systems for both the actual data processing entity and the individual who the data belongs to. One of the reasons for all these shortcomings is that not all systems are built on an overall and committed standard. Trustworthy computer systems and infrastructures are still missing. Thus, there is a lot of research work to be done on the future of identity management systems and their contribution to privacy.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 7. User centric standardisation 6. Preservation 9. Technologies for security
IPI 3	**Development and integration of Privacy-enhancing Technologies (PETs) into ICTs.** Solutions to the aforementioned problems can be implemented by privacy-enhancing technologies (PETs)[16], which should enhance the state-of-the-art of ICTs (i.e. dominant on the market and in use in organizations) with respect to at least some properties related to privacy or informational self-determination. It is recognised that they themselves span another complex of challenges. Many building blocks for PETs have already been developed, but only few of them are available on the market until now. Thus, successful business models for PETs and for supporting infrastructures have still to be elaborated. As PETs will need to be integrated within an environment, there may be interactions and interdependencies with other system components, which influence security and privacy. This will require a certain degree of redesign within the system components. Even a combination of multiple PETs may lead to weakening rather than enhancing the degree of	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 7. User centric standardisation 6. Preservation 9. Technologies for security

[16] In this document, we use the term PET in a broad sense, comprising all privacy technologies which enhance the state-of-the-art (i.e. dominant on the market and in use in organizations) with respect to at least some properties related to privacy or informational self-determination.

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	privacy. Clear privacy metrics are missing. Also, an analysis of possible interdependencies between the use of PETs and other technological components and of related effects on the users' privacy does not exist, let alone ways to inform them appropriately. Such information would help to know additional precautions that a user has to take in order to assure his or her privacy. Privacy seal programs and audit programs for example should take into account that assumptions on the environment and its trustworthiness should be communicated to and understood by the users.		
DTI 1.	**Trustworthy adaptability.** (i) complexity of systems is growing out of control, amplified by the advent of ambient-intelligent pervasive and ubiquitous computing; more and more "always-on" complex systems are being deployed or planned, especially by governments; (ii) growing interdependencies between systems, services and humans; (iii) threats take advantage from complexity and interdependencies; (iv) as in nature, this requires adaptation towards a state good enough for survivability. It is a challenge/priority theme because: It requires innovative approaches such as proactive-reactive design under uncertainty, adapting functional and non-functional properties while providing guarantees on adaptation result, autonomous and decentralised system algorithmics, trustworthy monitoring and update for continuously-on systems. If addressed, this will contribute towards the widespread deployment of very dynamic and evolvable systems that can be trusted in spite of their complexity. In other words, where 'complexity' is not an excuse for 'undependability' as is the case today. If not addressed, there are a number of risks including a serious fallback on plans to realize the ambient-intelligent society; serious hazards in the operation of systems that alternate between states of fossilised dependability/security and periods of undependability/ insecurity during and after system changes.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures
DTI 2.	**Balanced trustworthiness** (i) various attributes of trustworthiness (reliability, security, safety, etc.) extremely difficult to estimate and predict; (ii) attributes emerging from combinations thereof, even harder. (iii) on the other hand, the perception of trustworthiness and hence the degree of trust may vary depending on which side of the fence we are in (e.g. DRM, TCPA). Is a challenge/priority theme because: • Achieving effective trade-offs between these is often required but unfortunately is a continuing even greater challenge. • Trade-offs between attributes (ex. availability and integrity, security and dependability), and trade-offs between what suppliers and users seek (e.g. privacy, control, etc.), are at the heart of this problem. If addressed effectively it will: • help answer questions like "How hard can we make it for a hacker to attack a system, and still keep the service price/usability attractive to a legitimate user?". • enable the provision and deployment of much more satisfactory systems and services. If not addressed, risks: • Technologies deployed will risk becoming part of the problems, rather than the solutions. • Systems approach to dependability will continue the road of patchwork, unfortunately seen far too often.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	A continuation of the present situation in which many systems provide a very poor balance of the attributes, e.g. high security at a great cost to usability		
DTI 3.	**Rethinking availability** Description: (i) Classical dependability based on aprioristic and all-or-nothing criteria. Availability has been designed-in by redundancy according to forecasted fault modes, and predicted/ contracted to the user upon deployment. (ii) Whilst remaining a crucial attribute of today's systems, the future will bring new variables that will invalidate this status-quo: dynamics, uncertainty, evolvability, mobility, energy, maliciousness, sharing of critical and non-critical operations. Is a challenge/priority theme because: This requires an approach where availability becomes itself an evolvable and survivable attribute, in essence conditioned by: evolution of the environment; oscillation in QoS of the infrastructures. However, guarantees must still be met in some form, and this is a hard research problem, encompassing technology and societal factors (such as managing user expectations). If addressed will: • Bring in a totally new perspective on the 24x7 problem equation in a world of threats, what we might describe as 'acceptable availability'. • Hopefully contribute to creating future infrastructures that are at least as resilient to crashes, overloads and attacks as today's systems are. If not addressed, risks: • Keep increasing the risk of operation of the current combined critical/non-critical infrastructure substrate. • Amplify this risk by extending it to edges brought in by ambient intelligence, like sensor nets, mobile gadgets, home networks, car communication, navigation assistance systems, etc.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures
SPI 1.	**Security Analysis.** Following the idea that "you can't control a system if you can't predict its behaviour", automatic security analysis methodologies and tools need to be developed. This must be focused towards predicting differences in behaviour of an attacked system. It must consider system functionality and performance, and must be able to generate not only technical data but also economical parameters (such as estimated loss per minute caused by a specific attack). The latter is very important to reconcile investment with potential damage and lays the foundation for the development of ICT risk insurance strategies. Moreover, international agreements already call for quantitative economical evaluation of ICT risks (e.g. the Basilea-2 agreement) and this will increasingly be the case in the future. Security analysis should be performed via system simulation and formal methods. There is not a clearly superior approach among them, and both should therefore be pushed because they are capable to catch different aspects of the security problem. Moreover simulation and formal methods may differ in the size of the manageable problem, and can also be used iteratively to validate each other's results. If effective security analysis techniques (be them based on simulation or formal methods) are not developed then we will be unable to predict the effectiveness of our security solutions perform and to perform a cost-benefit analysis. In other words, we'll continue to have qualitative analysis, rather than quantitative.	5. Development processes 8. Service-oriented architectures	5. Development processes 3. Availability 6. Preservation 8. Service-oriented architectures

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
SPI 2.	**High Level Policies.** Since "you can't design/configure a system if you can't exactly express your needs", we call for the capability to describe and manipulate high-level security policies. This is opposed to the current situation where security requirements are very vague, expressed in natural language and translated to the actual configuration of the protection tools by security technicians. On the contrary, a high-level language should be more close to individual needs and business logic, so that it can be adopted by final users (either citizens or ICT managers) to clearly state their protection requirements. Appropriate tools must then be developed to automatically refine the high-level policies into low-level security controls (security management). This in turn generates the issue of keeping the high and low level views synchronized, since day-by-day management tools typically work at the lower levels and could invalidate the design automatically generated from the high-level policies. Policies are also vital in cyberspace interactions, such as those that occur in P2P systems or e-commerce transactions, to automatically negotiate acceptable policy (and hence, a set of security parameters) with neighbours and the intelligent ambient. If a high-level policy system is not developed, then the protection systems will be prone to design errors (due to bad specification), difficult certification and audit, and complex interaction in open environments.	5. Development processes 7. User centric standardisation 8. Service-oriented architectures	5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures
SPI 3.	**System Modelling** Following the concept that "you can't protect a system if you can't describe it", it is required to develop models of the target system and the surrounding ambient, including users and applications. The description must include the system topology, the network and application functionality, the security capabilities and the user behaviour. Integration with existing partial views of the system (such as that used for network management and for inventory control) is important, as well as the ability to accommodate dynamic changes (for example of network filters or routing strategy). System model is vital to perform security analysis (SPI challenge #1) and to automatically deduct and implement controls specified by high-level policies (SPI challenge #2). In other words, it is the foundation to build automatic security management techniques. Moreover a correct system model, that includes security capabilities, is also relevant to any negotiation strategy when an agreement has to be found about protection parameters with neighbours and the ambient in general. If comprehensive system description capabilities are not developed, then we will lack the substrate for all the other activities and in particular we will be unable to perform rigorous quantitative work, be that related to security analysis or to automatic policy deployment.	5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security
SPI 4.	**Neutral Security Capability Language.** The top-down approach foreseen by the SPI could underperform if the protection tools used to implement the policy do not provide a full description of their capabilities, or if they use specific concepts or tools invented by a provider. To solve this problem, a neutral security capability description language should be created and security tools could provide proper hooks to implement some high-level functions without disclosing their proprietary or patented solution.	5. Development processes 4. Interoperability 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security

Challenge reference	**STF Challenge**	**Advisory Board Recommendations**	
		Medium term	**Long term**
SRI 1.	**Building in Security from the start of the process.** Security and trust in ICT have to evolve as part of internationally accepted standards applied across multiple systems to provide easier interoperability across end to end systems. In this context, development of guidelines of security and trust models to system designers should be encouraged, so that the systems are built with the security functions from the start. Security is very difficult to build as an afterthought.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 9. Technologies for security
SRI 2.	**Data Protection.** Privacy and data protection becomes more and more an issue with the powerful capabilities providing for relatively easy access to comprehensive information about both private individuals and intellectual property.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 9. Technologies for security
SRI 3.	**Security in Heterogeneous Environment.** ICT has heterogeneity in its end to end communication links processes. Equally, security functions provided by different operator networks vary. However, from the user perspective, they will need to be able to get end to end security and trust through interoperable networks and functions. Hence, number of challenges identified in the above sections addressing different initiatives form part of overall challenges to be addressed as security research framework, addressed by SRI.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 9. Technologies for security
SRI 4 (with input from IPI)	**Usability. (IPI)** A general problem of today's Security tools is that they may be too complex for most of the users, especially with regard to Privacy Enhancement Technologies. This is related to the fact that the complexity of legal regulations on privacy and of ICTs themselves has grown over the last years. Thus, reduction of complexity and enhancement of usability play an important role for their distribution. In particular, it is an unresolved problem until now to determine the best ways to impart an integrative view on the private sphere of the individual and to support the user in making decisions concerning the release of personal data. Here, not only technologies may be employed, but also the service of other parties can help in this matter, e.g. by providing appropriate configuration files or by acting as intermediaries on behalf of the user if desired. E.g., in the security field there is a good tradition of Computer Emergency Response Teams (CERTs), which inform about security incidents and the countermeasures that have to be	1. Empowerment 5. Development processes 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 9. Technologies for

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	taken. People may need additional organizations, which inform them about “privacy incidents”, i.e. events, which may affect their privacy, and give advice how to react in order to maintain their private sphere. As acceptance and user-friendliness of PETs is important, appropriate user models and user interfaces should be elaborated. (SRI) Usability of security features developed and built into the system are the key factors in providing the user with the control of security and privacy and for his data protection. This issue is not well addressed (or not even considered) by the vendors and service providers. The challenge is to understand user behaviour in the contextual environment and provision appropriate measures.		security
SRI 5.	**Cost Effectiveness.** Cost effectiveness of security and trust is another key challenge, which balances the level of security that can be provided at the reasonable cost. The security and trust of ICT is always related to the business risk assessment. Optimisation between the costs and security measures has to be managed.	5. Development processes 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 9. Technologies for security
SRI 6.	**Citizen Empowerment.** In many cases, users themselves will have to manage their privacy preferences. They should be supported by technologies for self-management (among others: identity management systems), which empower them to assert their rights. The inclusion of “privacy control functionalities” such as negotiating privacy preferences, managing the consent, access and even correct or delete individual data processed by the data processing entity according to the applicable laws would enhance ICTs tremendously. The field of ambient intelligence needs solutions for the informational self-determination of individuals, i.e., providing all necessary information and choices with respect to one’s private sphere. How to achieve multilateral security in ambient intelligence is an open issue especially because personal information may be transferred to devices the trustworthiness and security of the device is not known and often times questionable. In these cases classic PETs and “privacy control functionalities” are lame ducks. We need new mechanisms that ensure that personal information continues to be protected once it has been given away.	1. Empowerment 5. Development processes 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 9. Technologies for security
SRI 7.	**Legally compliant systems.** Designing legally compliant ICT systems is a challenge as well, especially in an international context with potentially numerous regulations, which even may be contradictory. Changes in legal regulations, as e.g. announced in the area of data retention, lead to updates or even redesigns of ICT systems. In particular where privacy law or privacy principles are affected, a careful development is necessary, e.g., to balance the demands of privacy and law enforcement. For biometrics, a careful evaluation of methods for verification or identification with respect to privacy is still necessary. In particular, side effects such as the possibility to disclosing medical or other unnecessary data for authentication purposes has to be elaborated. The possibilities of authorized law enforcement access to data by law enforcement officials need to be developed in a way that minimizes the invasion of privacy and guarantees the individual’s privacy principles. For instance, monitoring should be done on an isolated-case level rather than for all users of a system. Similarly, surveillance and monitoring methods, e.g., for criminal incidents, have to be developed, which are not privacy-invasive for individuals not involved in the recorded incident.	1. Empowerment 5. Development processes 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 9. Technologies for security
SRI 8 (input	**Creating awareness (IPI)** (IPI) Research should be conducted on metrics of privacy, which not only help in estimating the degree of privacy implemented within an ICT system, but also can be used to illustrate privacy-relevant	1. Empowerment 7. User centric	1. Empowerment 7. User centric

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
from IPI).	parts and risks in PET user interfaces. False, incomplete or imprecise data including derived profiles and scoring values which are interpreted to predict the future of an individual may be an own focal point within this field. Socio-economic factors should be investigated as well, e.g., in developing business models or performing acceptance studies. Best practice cases for PET building blocks such as convertible credentials should be elaborated. In addition, psychological and sociological research should be performed for privacy, e.g., to get a better understanding on what motivates people to release data and to give better feedback to European citizen on the consequences of data released. Prototypes in the communication area are useful for users to experience the consequences, as giving away data here often results in more incoming communication (e.g. emails or other messages). So users can get a quick feedback with respect to their choices and the consequences. By following these approaches, the goal of improving the business position for ICT companies in the EU will be reached by building trust and user acceptance. We are envisioning data protection features and the usage of PETs as a quality “trademark” for ICT solutions in Europe, which can also be used for supporting the export of European solutions. The main objective is to enhance the image of the ICT development processes (and ultimately of the solutions) by integrating secure identity management and data protection mechanisms already in the design process of ICTs ie. data privacy by design	standardisation 9. Technologies for security	standardisation 9. Technologies for security
SRI 9 (input from IPI).	**Behaviour of people with regard to Security and Privacy. (IPI)** There are considerable differing views on the user’s perception and level of importance for privacy protection in situational settings. There have been studies in which the respondents rate privacy with highest importance, but, on the other hand, there are a lot of reports and observational studies that show how easy people give away their personal data without a second thought. Sometimes people are surprised and astonished about the amount of personal data that has been collected and stored about them. Research on the motivational factors behind this “irrational” behaviour would help ICT developers to build in expected and assumed privacy functionalities.	1. Empowerment 5. Development processes 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 9. Technologies for security
v6SI 1.	**Dependence of the deployment of IPsec supported by a PKI infrastructure.** Similar to IPv4, IPv6 will depend on good deployment of the PKI Infrastructure.	5. Development processes 3. Availability 4. Interoperability 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 9. Technologies for security
v6SI 2.	**Motivational aspects of security vendors.** The second challenge is the motivation of security vendors to move to deployment of IPv6 which would require redesign of de-perimetarisation of the firewall concept. This effort requires a solid business case.	5. Development processes 3. Availability 4. Interoperability 7. User centric standardisation	5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
		9. Technologies for security	standardisation 9. Technologies for security
v6SI 3.	**Acquisition of new security knowledge.** The third challenge resides in the acquisition of new security knowledge to enable security engineers to write new lines of code that need to be tested and smoothly integrated into production networks without introducing new vulnerabilities. The perception that IPv6 is not a security panacea adds more to the fear and resistance to try new security concepts. IPv6 cannot indeed protect against misconfiguration, poor application design or poor security design. It cannot remove the need for vigilance and a pro-active approach to network security. However, IPv6 can help to raise the baseline of security for networks today. IPv6 technology can improve enterprise security, thereby protecting revenue. It can improve the security of public access networks, like Wi-fi hotspots, thereby minimising outages and customer dissatisfaction. IPv6 can provide better communications privacy than IPv4. The efficiency and security of IP mobility deployments can be improved with MobileIPv6, thereby reducing costs for operators. IPv6 can also minimise exposure to port scanning providing defence-in-depth and further protecting revenues and investments for both operators and end-users.	5. Development processes 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 9. Technologies for security
SVPI 1.	**Enrichment of semantic cooperative standards.** There is a need for new enriched semantic-cooperative standards to define the security models and protocols (security context and personalised policies to observe within each such context as defined by the user) including those relevant to web services and smart proxy-enabled security context-sensing, context-sensitive accountabilities, security policy, model and protocol appropriation.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security	1. Empowerment 5. Development processes 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security
SVPI 2.	**Virtual communications domains.** A new breed of communication management (including middleware) will be needed along with more expressive semantic-cooperative service description and session configuration resolution to hide the complexity of security-context-aware personalised privacy and security protection from both the user and the application layer. This is to support the ***modelling and inter-operation of*** virtual communications domains across whose boundaries scalable context- aware security and trust services could thus be invoked in a graceful, dynamic and seamless fashion. It is crucial to examine the pre-requisites to underpin the virtualisation and semantic architecting that is required to enable the graceful integration of various security technologies, including legacy, evolving or new technologies.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security	1. Empowerment 5. Development processes 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security
SVPI 3.	**Architectural Challenges.** Whilst the virtualisation paradigm powerfully underpins the Open Metropolis and multi-layer security protection objectives, it, at once, implies and supports significant other architectural capabilities whose availability within each trust domain and security context would significantly add to resilience of the security	5. Development processes 4. Interoperability	5. Development processes 4. Interoperability

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	protection; so ideally, we aim for additional virtualisation-enabled capabilities for efficient and effective: • S&T threat scenario situation assessment • S&T threat scenario pre-emption & threat chain breaking • S&T threat scenario forecasting, simulation, socially intelligent fixes & failure recovery policies enactment S&T threat pre-emption eco-system (immuno-genetic modelling) to combat the attackers' eco-system i.e. match the attacker's re-learn-re-innovate-re-attack chain so as to enable enhanced pre-emption, prevention and recovery in a dynamic attack environment	6. Preservation 9. Technologies for security	6. Preservation 9. Technologies for security
IISI 1.	**Novel trust and security models for the internet.** The Internet technologies of the future will be charged with securing the Internet layer issues of content integrity and confidentiality. Research will largely focus on developing novel trust and security models for the Internet and for the interoperable ubiquitous computing environments that exist today and for those in the future. Such security models would involve defining new mechanisms to provide confidentiality of Internet content, to provide secure authentication. There is also a requirement to obtain stronger and more reliable procedures of accounting and non repudiation of future Internet content handling, in particular with future e-commerce applications. Research here will focus more on advanced cryptography designed specifically for multimedia content and e-commerce applications.	5. Development processes 4. Interoperability 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security
IISI 2.	**Security and Reliability in home internet connectivity.** New avenues of research will need to be undertaken to provide not just security but also reliability in home Internet connectivity with the advent of prominent intelligent ambient devices. Security network management of these future home Internet devices will be addresses to assure security and safety is utmost across devices with different security capabilities. Due to the fact that so many objects of the future will become interconnected, researchers will need to direct their efforts to ensure that there is a protocol or standard in place to develop scaleable Internet security technologies across different platforms.	5. Development processes 4. Interoperability 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security
IISI 3.	**GRID Security.** There are numerous complex challenges in making GRIDS secure and trustworthy. Some of the problems are serious challenging as they require a high level of abstraction across very different technologies and areas of competence.	5. Development processes 4. Interoperability 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security
IISI 4.	**Secure Code development.** Secure code development will be vital to defend the Internet protocols from code exploits (buffer overruns and so forth). Both Internet code management and code risk analysis standards and methods will need to be developed to ensure that the code (largely FOSS based) is able to withstand new environmental threats. Secure Internet code management will incorporate new mathematical proof methods that will help verify and certify code is correct for its intended operation.	5. Development processes 8. Service-oriented architectures 9. Technologies for	5. Development processes 3. Availability 6. Preservation 8. Service-oriented

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	The future Internet security layer will provide many challenging research areas open to the European knowledgebase to solve in order to provide secure, reliable and always on ubiquitous Internet environment.	security	architectures 9. Technologies for security
IISI 5.	**Decisions regarding existing State of the Art.** The Internet layer will take existing state-of-of-the-art Internet technologies and decide either to build upon and extend these standards or to develop completely new standards that better describe a new internet movement based on past and current experiences. Such components to be addressed are current secure and authentication protocols such as IPsec, SSL and so forth. Can current secure code development standards be extended or do we need to re-develop new standards? Research will also look at existing methods of code verification and how best to build upon those methods and standards.	5. Development processes 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security
ASI 1.	**Global Application Security Processes in the development of Application Level secure systems.** In order to increase the security and dependability of the Application layer and to ensure application compliance and measurement quality, the developers must be properly trained and they must follow a global application security process, with phases that follow closely the application development phases from the idea/proposal/mandate phase through to the disposal phase. One of the major challenges is to develop scalable application level secure (AS) systems. Not only must the AS systems be scalable but they must be created in a way that provides a solid measurement of quality of service. In achieving these goals, proper code analysis must be undertaken that leads to secure code development in a standardised way. The end goal is to have a QoS security service that is scalable and is resistant to attacks in particular Malware and Spyware epidemics.	5. Development processes 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security
ASI 2.	**Application level security services in a distributed web enabled environment. (Interrelated to IPI, Biometrics, IISI, SVPI challenges)** (Interrelated to IPI, Biometrics, IISI, SVPI challenges) Applications running in pervasive and ambient intelligence environments must be capable of providing always-on mobile security and privacy. Significant research must be carried out to enable the applications to work with the new technologies being developed in the identity and privacy management areas, biometrics and internet infrastructures areas. For example, authentication and identity management systems in service-oriented architectures (SOA) built on Web services. Web services are essentially decoupled applications and the identity management is part of the underlying infrastructure. Therefore, in this domain, we are focused on dynamically responsive Security and Trust Chain service provisioning, which can hide the complexity of context-aware personalised privacy and security protection from both the user and the application layer. In order to accomplish this, there will need to be three virtual communication domains across whose boundaries scalable security services could be invoked to manage a user's dynamic Security and Trust chain in the context of user's business logic and value chain. Therefore, for each such client device/user, three interacting domains are virtualised to include all hardware and software modelled under each of: 1. Self-Domain (S): All HW/SW constituting user's personal client devices: home computer, office computer, laptop, PDA, mobile phone and native applications running on them (calendar, diaries, profilers etc). 2. Others-Domain (O), All HW/SW belonging to all other parties transacting with the user including that of peers and grid-enabled services. 3. Smart-Middleware-Domain (M): Any component involved in mediating data exchange across the boundaries	5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	between the above two domains. Thus, there are key research challenges arising from the need for graceful and reliable integration of the above virtualised environments within a secure, efficient, service-oriented, application centred, model-based, context-aware and event-driven computing environment		
ASI 3.	**Adapting traditional security frameworks to OSS development methods.** Open Source Solutions (FOSS) needs to be secured, but it needs a specific focus. Particularly in the public Sector, FOSS is considered a critical component providing a way to improve: • Transparency • Sovereignty • Ease of experimentation • Open Sharing of knowledge. Security in Open Source used to be a minor concern for two very different reasons. On one side, most of the Open Source applications were not seen as "business critical". On the other side, Open Source Infrastructure applications (mail, web server, routing, DNS, ...) had been around long enough to be run under the gauntlet of various security attacks to be now quite secure. Moreover, with a development model that enables and encourages source code scrutiny, there is a general feeling that security issues are easier to spot and to solve by the community. But with the wide adoption of Open Source solutions, the quantity of code to look at has grown significantly and the number of applications that are business critical has grown proportionally also. Moreover, new issues like Cross-Site Request Forgeries (CSRF) or (Cross-Site Scripting) XSS attacks are appearing at the application level. This leaves the FOSS world with issues of accountability and certification, and normalisation of architecture. A major challenge will be adapting traditional Security Frameworks to the Open Source development methods. Trying to solve these using conventional processes will most probably not work, trying for instance to demonstrate that a specific firewall meets specific security requirements is not a trivial exercise. Therefore, the FOSS communities should adapt the process they already very successfully use to develop applications to also manage the security issues of their applications, and applications interactions/architectures. Much of the FOSS success is linked to the way FOSS infrastructures are built: what is commonly referred to as "FOSS relies on the collaboration of the Cathedral and the Bazaar to build a city". We needs to build a framework where the security needs of an Architecture can be modelled, defined, reviewed in an open and transparent manner, using the same "Forges" the application development already use. Basically defining a "contract model" between application elements, thus enabling not only the collaboration of application developers within a comprehensive framework but also the collaboration of service providers on a live application. The goal is obviously not just to guarantee that an architecture «can» be secure, but that the specific way this architecture is run is secure.	5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security
MScI 1.	**Response time of Standards development process.** *It is interesting to note that the ISO SC37 WG6 is developing standards on cross jurisdictional and societal uses of biometrics.* Is the standards development process able to change and respond to the new changing paradigm on current challenges to the Security and dependability community, which can be summarised as: • From perimeter protection to the holistic, integrated system security • From central access controls to decentralized usage control	3. Availability 7. User centric standardisation 4. Interoperability	3. Availability 7. User centric standardisation 4. Interoperability

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	• From patch management on demand to long-term sustainable security • From security as a product to security as a dynamic process.		
MScI 2.	**Shorten time of Standards development process.** Current security standards development is a long process covering from 2 to 5 years. There is a fast track approach, which takes from 6 months to 1 year. There is a real need to shorten the time it takes to develop a consensus on a standard within the ISO world. W3C, IETF, ITU, ISO etc. are all working on identity and integrating the concept of identity into certain standards. Liaisons between the different organisations are, mostly, in place. However, strong liaisons have not always been established with ISO SC37 Biometrics and this shows that the existing ways of working together are outmoded, outdated and take too long. For example, ISO takes at least 30 months to fast track acceptance of a standard. New ways of working must be found to bring the standards process into tomorrows world. IF NOT ADRESSED, this will continue to be extremely inefficient process.	3. Availability 7. User centric standardisation 4. Interoperability	3. Availability 7. User centric standardisation 4. Interoperability
MScI 3.	**More Community participation to standards bodies.** There are currently very few participants from the user community, especially from SME sector (availability of English speaking personnel) and New Member States of the European union (cost factor and lack of resources of the national standards body). Most existing participants come from universities or industry. The liaisons between the different standards organisations are not always clear cut, and even within ISO, there can arise divergence on who is responsible for what. Currently, there are three sub committees which are working on security SC37(biometrics), SC27 (security methodology & process) and SC17 (cards). Amongst the European countries, there is only the UK that doesn't charge for participation in the standards body - BSI IST/44 biometrics for example. So this is a barrier stopping qualified professionals from participating in the International Standards organisation process. If not addressed, a real European contribution to the standards process will take far longer to build.	1. Empowerment 7. User centric standardisation	1. Empowerment 7. User centric standardisation
MScI 4.	**Security Certification major growth area.** Certification in security of products, people and companies is a new field and a major growth area. For example, there is still no European test centre for biometric vendors, and most countries have yet to agree a certification centre for ISO17799 (security methodology) or ITIL (BS15000) (service management of IT systems). The most important challenge in identity security is in the interoperability of biometric vendors products. The ISO19794-2 standard has just been published together with 3 others. Currently, no vendor can declare themselves conforming with this standard, there is no accreditation of European laboratories from the national bodies such as UKAS in the UK. The MIT project will begin in January 2006 and to some extent will move forward in this area. It is hoped to have certification of vendors at the end of 2006 but ID cards and passports are already being issued with non-interoperable biometric algorithms. Therefore, by 2007-2008, we should have the beginnings of an healthy European certification industry for interoperable biometric algorithms and sensor devices. BUT WHAT ABOUT THE REST OF THE SECURITY INDUSTRY ?	4. Interoperability 5. Development processes 6. Preservation 7. User centric standardisation	4. Interoperability 5. Development processes 6. Preservation 7. User centric standardisation
WSI 1.	**Convergence.** The future is all about Convergence, which brings forth an environment with new requirements and challenges and evolving standards, which only define a part of this since any of the disruptive technologies come from industry fora. 35% of current Telco suppliers are IT companies. This percentage will increase in the future- it also means that security procedures defined in the Telco standards do not and will not apply in the future. The ″Rules″ are changing. So Policy known today need not apply tomorrow. How do we still maintain Privacy and the Telecom laws to	4. Interoperability 5. Development processes	3. Availability 4. Interoperability 5. Development processes

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	avoid regulatory conflict.		
WSI 2.	**Definition of Optimal security roadmap.** It is clear there is a need to give Security the highest priority. However, can this lead to overly secure concepts? We need to find the right balance in defining the future so that FP 7 can offer enough of interesting mid- and long term topics for research and that Projects produce valuable results for the standards and Industry to commercialize on.	1. Empowerment 3. Availability 4. Interoperability 5. Development processes	1. Empowerment 3. Availability 4. Interoperability 5. Development processes
WSI 3.	**Integration of existing technologies. .** A number of Security Solutions already exist. Most of these have been either deployed or are innovative proposals out of research and new industries. However, there is also a lot of repetition or very similar solutions yet leaving holes in between that haven't been addressed. The challenge here is, how do you harmonise these to avoid additional cost and performance loads deficiencies on the network. For example, how can carriers/operators efficiently make use of the solutions-eg, USIM/ISIM. The challenge is to map the transition steps towards the future?	3. Availability 4. Interoperability 5. Development processes 6. Preservation 9. Technologies for security	3. Availability 4. Interoperability 5. Development processes 6. Preservation 9. Technologies for security
JW1.	**Secure data management, and synchronization and private exchange of user profile and context information.** One of the future challenges for FP7 is a paradigm shift of gradually replacing the physical boundaries with logical boundaries maintaining context in order to move from a system-centric, or "Central-Command-and-Control" to a Citizen-centric, or "Empowerment of the Citizen" Approach to security. This view advocates a shift from global identification (database silos) to a context-specific local recognition (persistent logical identity boundaries determined by context) and the elimination on the dependence of compliance management to focus on sustainable security through citizen empowerment (giving the citizen the power to control their data. Few ICT technologies have been designed with this kind of scenario in mind so a gradual process of revisiting basic technologies is required to ensure that the context sensitive empowerment of the citizen is supported. The transformation will be much more than a quick fix and will require a sustained effort on all R&D levels to ensure understandable, interoperable, secure, convenient and efficient systems.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 7. User centric standardisation 6. Preservation
JW 2.	**Efficient encryption and cryptographic mechanisms and algorithms suitable for different types of devices and networks.** Cryptology research continues to deliver a stream of important results, but work must continue to keep abreast of trends in network volume and performance, and of the development of new attacks and insights into vulnerabilities. When we evolve to an ambient intelligent world, privacy concerns will increase and cryptology will need to be everywhere (even in the smallest devices). This means that cryptology will be needed that can offer acceptable security and performance at very low cost (hardware footprint, power consumption). Cryptology will be needed to distribute trust and to reduce the dependence on a single node. Challenges also include the need for very long term protection of sensitive or contractual records, and preparedness of the possibilities of quantum computing.	5. Development processes 4. Interoperability 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 9. Technologies for security
JW 3.	**Secure software and execution environment including O/S.** The requirement may be divided into three levels: the trusted hardware to physically execute software; the trusted operating system that together with the trusted hardware provides the interfaces (APIs) available to operational software; the software itself which may be divided into two further classes (i) trusted, verifiable system software for, say, execution of cryptographic algorithms, secure protocols, and user interfaces, and (ii) trusted application software to deliver functional services. A further class of un-trusted software must also be provided for (sand-boxes etc.), whilst maintaining strict protection of the rest of the system. In addition to the design, implementation, and validation tools to deliver these, there is also the need for	5. Development processes 4. Interoperability 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented architectures

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	comprehensive modelling tools and environments to provide large scale simulation of design and of validation scenarios. Research is necessary into more economical and practical ways of providing trusted components and systems. The delivery and deployment into real operational networks, services, and terminals also still need much investigation, prototyping, and assessment. There are very serious issues here about how to preserve and utilise the current legacy of operational software with its multiple patches and its known deficiencies in terms of design and implementation rigor and the impossibility of full validation. Other specific issues include: management and maintenance (e.g. upgrade) of certified software; the roles of the smart card in general and the SIM in particular; relationships to privacy and DRM; *trust* (q.v.), the need for automatic security evaluating tools during development process, and achieving truly high quality software - despite the large gap between best practice (and research) and industry average. Mobile service and OSS design must include up front security and privacy management, into service specification, instead of the current day approach as an "Add On". There is a need to enable the SW designers and security experts speak the same language for security specifications, or more specifically, have consistent and comparable expectations. There is a need for modelling security requirements: Analysis, Validation, etc. and a need for making SW applications dynamic ie. build context awareness into application		9. Technologies for security
JW 4.	**Identity management & privacy.** One aspect of this topic concerns the mechanisms for user identification and authentication, and the means to protect users' credentials and sensitive information from unauthorised disclosure or manipulation; this is covered by **JW2** and **JW3**. The other aspect is the user expectation for privacy: the right to remain anonymous or unidentifiable in appropriate circumstances, and the ability to retain control, or at least influence, over the handling of personal or sensitive information released in confidence to other parties. There are two parts to this second aspect: the technical issues, potentially within the scope of **JW2** and **JW3**, again; the other part concerns the sociological and political issues arising, not least the ongoing tension between the legitimate rights and wishes of the individual, and the needs of society in its responsibilities to protect and benefit its members as a whole. Two specific concerns arising in this area are: the need for legal interception in pursuit of law-enforcement, and with it the unease about abuse of the technical capability both by the authorities and by the unauthorised criminal; the second concern relates to the ability to build quite intimate personal models or profiles from apparently innocent scraps of information with a view to circumventing inadequate privacy protection – technical or procedural. A further topic that should referenced here concerns the current distrust by the subject – arising from an apparent over-confidence or reliance by the authorities – in the true effectiveness of bio-technology as the basis for identification. Its usefulness as a *component* of an overall identification scheme – or schemes – is welcomed. The main questions relate to vulnerability to identity theft and masquerade, as well as the basic fallibility of some current proposals	1. Empowerment 5. Development processes 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 9. Technologies for security
JW 5.	**Secure and dependable end-to-end network protocols and applications enabling a simple-to-use trusted transaction environment.** Research and business experimentation into managed security and privacy services, in mobile space, to create incentives turning burden/costs into opportunities is needed. It should be context aware and with dynamic reconfigurability/control so that the trusted environments and the hostile/volatile environments can be distinguished and be dealt with accordingly. Other challenges for e-2-e Security with mobility include secure neighbour discovery, MIPv6 and AAA integration, interdomain issues, and Key management. Security in sensor networks and rule based support of pervasive use of private protection.	1. Empowerment 5. Development processes 4. Interoperability 8. Service-oriented architectures 9. Technologies for	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
		security	architectures 9. Technologies for security
JW 6.	**Unified Digital Rights Management environment.** There is a need for an EU-based approach for digital rights management to enable the EU to become a more effective content creation and provision environment. In order to accomplish this to the benefit all of the stakeholders involved, it will be necessary to provide an framework and environment with protocols that will enable the traceability of the rights all the way back to the contents rights owner. There needs to be a proper balance between the rights of the producer, those of the supplier and the purchaser/user. Some of the technical approaches include included ontologies, asset identification, perceptual hashing and semantic linkages for traceability. These would have to cope with content that is changed throughout the whole chain ("who owns what and when") and the ability to observe the adherence to agreed rights. Best efforts must be made to enable transparency in rights distribution, and/or creation of DRM distribution networks. Addressing these challenges within FP7 could open up very new and exciting opportunities for special actors within this high growth potential area.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 9. Technologies for security
JW 7.	**Transparent and flexible Service Level Agreements.** One of the long term challenges is to replace the current (unjustifiably trusted) system creation environment with an end-user based environment, which elicits their trust in a more proactive manner. This should be based on negotiation (or enforceable and sanctionable SLAs) between the end user and the provider in order to match the end user needs and their tolerable risk assessment criteria levels. This is considered a long term challenge because it cannot be done without revisiting, harmonising, changing and/or replacing the various approaches in use today. Currently, there is a lack of trust metrics to establish/define quality of trust and a well defined Standardised Trust Management model is needed with quantifiable metrics models for Security and Trust.	1. Empowerment 7. User centric standardisation 8. Service-oriented architectures	1. Empowerment 3. Availability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures
JW 8.	**Combined multi-layered mobility support and authentication/authorization across diverse networks and support of simultaneous use of multiple access technologies.** Security for mobile services, which is independent of underlying access networks, will require seamless handovers requiring negotiations of new SLA. Virtualisation Interoperability standards are needed and heterogeneity requires flexible solutions and this flexibility opens holes in the systems and the attackers easily find the weakest links.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security
JW 9.	**Device and network protection against attacks (virus, Trojan, DoS, Phishing) and intrusion detection.** Threats and vulnerabilities have to be identified and should be addressed based on level of security needed and user/application profile in an auto configuration mode, so that users get more trust in the network and applications. Such functionality will raise the trust among the users.	1. Empowerment 5. Development processes 7. User centric standardisation 9. Technologies for security	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
			standardisation 9. Technologies for security
JW 10.	**Safe and secure software download enabling networks and device re-configurability.** Dependability issues in safe/secure downloads must be addressed. Some of the issues include intelligent function firewalls, intelligent access controls, need for user friendly download and building up of software trust and risk awareness. There is a need for dependencies and security maps to provide traceability and to keep the users informed of what is happening and automatic reporting mechanisms should be in place.	5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security
JW 11.	**Mobile connectivity/integration to the GRID community.** Another area of significant interest raised at the Joint Mobile and Wireless Security and dependability workshop was the future interrelationships and interactions between the mobile and wireless and the Grid communities. Security of today's large scale, open, distributed heterogeneous systems (such as computational grids, peer-to-peer systems, pervasive/ubiquitous computing, etc.) has become a mainstream operational concern. Establishment of in-depth security services and trust relationships are the most desirable features for such systems. In a Grid environment, where identities are organized in VOs that transcend normal organizational boundaries, security threats are not easily divided by such boundaries. Identities may act as members of the same VO at one moment and as members of different VOs the next, depending on the tasks they perform at a given time. Thus, while the security threats to OGSA fall into the usual categories (snooping, man-in-the-middle, intrusion, denial of service, theft of service, viruses and Trojan horses, etc.) the malicious entity could be anyone. An additional risk is introduced, when multiple VOs share a virtualized resource (such as a server or storage system) where each of participating VOs may not trust each other and therefore, may not be able to validate the usage and integrity of the shared resource. Security solutions that focus on establishing a perimeter to protect a trusted inside from an untrusted outside (e.g., firewalls, VPNs) are of only limited utility in a Grid environment[74]. Conventional Grid Paradigm constitutes of secure dynamic virtual organizations relying on rather reliable networks accessible without any preconditions where users and resources are tight to a given location and network address. The context of a member of such a kind of collaboration is considered to be static and more or less equal to the one of all other collaborators. Context information such as device capabilities or available bandwidth is not considered. Next generation of Grid will have to allow its participants to be mobile. This includes nomadicity, change of network services provider during a session, support for device or session mobility, etc. Mobile Grid will offer a number of features to its users; however, its security design will become more complex as it will inherit all the security vulnerabilities of the mobile world. The security designers need to keep in their minds the intrinsic nature of both Grid (large scale distributed computing) and mobile worlds to come up with some adequate solutions.	5. Development processes 4. Interoperability 8. Service-oriented architectures 9. Technologies for security	5. Development processes 3. Availability 4. Interoperability 6. Preservation 8. Service-oriented architectures 9. Technologies for security
JW 12.	**Meta security policies for independence of networks. Meta security policies for independence of networks.** The goal here is to create a generalised framework for specification of security policy that provides for specific application	5. Development processes	5. Development processes

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	and interpretation at real implementation levels irrespective of local technologies, so as to create coherence and consistency within a domain. It also allows for creation of co-operating policies between domains.	interoperabilty 7. User centric standardisation 8. Service-oriented architectures	3. Availability 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures
JW 13.	**Virtualisation at architecture level.** Research fundamentals include the overall architectures at both the conceptual or virtual level, for high level design, modelling, and policy making, and at the real level concerning the working, functional entities and interfaces, and the communications between them. The requirements are for seamless roaming and interoperability in a dynamically shifting environment composed of a heterogeneous set of entities and services. At the network level, overlays – again dynamic – will deliver a wide spectrum of user needs. The challenge is to identify a sufficiently general set of architectural components or building blocks and to specify their functionality, interfaces and the protocols that govern their intercommunication and interoperation. Ideally, we should aim for additional virtualisation-enabled capabilities for efficient and effective: • threat scenario situation assessment • threat scenario pre-emption & threat chain breaking • threat scenario forecasting, simulation, socially intelligent fixes & failure recovery policies enactment • self-x properties: – self configuration. – self organisation – self protection, – self defence, – self “healing”, threat pre-emption eco-system (immuno-genetic modelling) to combat the attackers’ eco-system i.e. match the attacker’s re-learn-re-innovate-re-attack chain so as to enable enhanced pre-emption, prevention and recovery in a dynamic attack environment.	5. Development processes 4. Interoperability 6. Preservation 9. Technologies for security	5. Development processes 4. Interoperability 6. Preservation 9. Technologies for security
JW 14.	**Seamless interoperability.** The appearance of seamless inter-operability could be achieved through a very large set of carefully specified bilateral agreements between communicating entities, or as a result of an architectural approach that results in sets of standard specifications for entities and their inter-relationships. This could then become a by-product or development of virtualisation at architecture level, as described above.	4. Interoperability 7. User centric standardisation 8. Service-oriented architectures	4. Interoperability 3. Availability 7. User centric standardisation 8. Service-oriented architectures
JW 15.	**Attack Resistance.** Although this should be an aspect of many of the other challenge-items, it is important enough of itself to be separately identified. In addition to the development of counters to known, classic attacks, new attacks and vulnerabilities resulting from the expansion of the networks will be inevitable. Pre-emptive analysis can prevent some potential attacks through specific defences or avoidance. Defence against others may be possible as a result of the development of generic defensive approaches and strategies – ubiquity and redundancy. As back up to deployment of counters to attacks, there needs also to be parallel development of resilience strategies that provide for successful, rapid	1. Empowerment 5. Development processes 7. User centric standardisation 9. Technologies for	1. Empowerment 5. Development processes 3. Availability 4. Interoperability 6. Preservation

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	recovery following disaster, whether this be as a result of attack, malfunction, defective design or implementation, or just plain fat-finger problems.	security	7. User centric standardisation 9. Technologies for security
JW 16.	**Radio Access Network, Core Network and Service architecture.** There are also security and dependability requirements for Software Defined radio (SDR) including issues involving spectrum optimisation, the need for flexible services, certification of SDR platforms, local regulation on cryptography use, standardisation of SDR services and protocols, which are highly challenging because one has to balance the 'openness' and the 'controls'.	5. Development processes 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security.	5. Development processes 3. Availability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security.
JW 17.	**Cryptology.** In order to protect information stored or transmitted outside of a 'home' trusted environment, and even to provide certain trustworthy interfaces within that trusted home, specific challenges for cryptology research include[73]: • *Crypto-everywhere*: software, hardware, and nano-scale implementations will be required as cryptography is deployed as a standard component of all communication and computation layers and – with ambient intelligence (or pervasive computing) – at "every" physical location. Requirements will be for lower cost, higher performance, specific applications, smaller size, low complexity, provable correctness, and low energy consumption. • *Long-term security*: Many crypto-systems considered robust have been broken after a certain amount of time (between 10-20% years). For instance, most of the hash functions developed before 1993 have been broken. We need to build crypto-system that offer long term security, for example for protecting financial and medical information (medical information such as our DNA may be sensitive information with impact on our children, our grandchildren and beyond). In the medium term, we need to be prepared for the eventuality that large quantum computers could be built: this would require an upgrade of most symmetric cryptographic algorithms and a completely new generation of public-key algorithms. • *Provable security*: cryptography has been very successful in developing security models and security proofs within these models based on a limited set of assumptions but more work is needed to expand this approach to more areas in cryptology; automated tools to assist in developing and checking such proofs seem a promising research direction. • *Secure implementation*: even if we are able to get theoretically sound cryptographic algorithms and protocols, most of their failures can be found at the implementation level. A design methodology and technical solutions to increase resistance to side channel attacks (power, radiation, timing attacks) and work on secure APIs would be very relevant. • *Digital rights management*: several techniques such as fingerprinting and watermarking are available and there is a growing interest in this area. However, there is a lack of solid scientific basis (even just openness about techniques used in commercial products) and insufficient academic research. *Privacy*: diffusion of sensing, location based services, explosive growth of storage capacity and communication mechanisms, and data mining technologies present a major risk to privacy. The problem lies in the asymmetry of technology: advances in technology make privacy violations much easier, while protecting privacy is complex and delicate (integrated solutions are necessary that work at all layers – physical, network, transport, application). Ease of	5. Development processes 7. User centric standardisation 9. Technologies for security	1. Empowerment 3. Availability 9. Technologies for security

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	use plays an important role here too. Advanced cryptographic protocols can bring substantial advances in this area		
JW 18.	**User Empowerment.** This was a major topic of interest at the **"**Trust in the Net**"** Conference held in Vienna on 9th February 2006 [75], and has been reiterated constantly within the STF and Advisory Board (see Section 2.4, above - specifically Recommendation 1, and Section 8.4.3 - specifically **SRI6** – *citizen* empowerment). The need for user involvement on security and dependability arises from two distinct sources. The *first* is the user expectation of having appropriate control over personal or sensitive matters. Here the question is how to assign appropriate controls to the individual, as opposed to all controls being centralised in either major providers of choice – banks, Service Providers, etc.(discretionary), or monopolies – .gov, NHS, etc. where there is no choice.(mandatory); The issue is the general need for the user to be in control of its own information and resources, or rather the fear of not being in control: that, without the user's awareness, let alone permission, commercial, governmental, or criminal agencies may gain unauthorised control or knowledge of the user, possibly by aggregating seemingly harmless fragments (see **JW4**, above). The *second* is as a consequence of the deperimeterisation that arises from the evolution of dynamic network architectures: appropriate controls will need to be vested in the individual, while some must remain the responsibility of certain service providers, and others, relating to physical aspects and operations, must necessarily be retained by the operators of the communications networks or their agents.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security.	1. Empowerment 3. Availability. 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security.
JW 19.	**Usability, Security, Trust and Dependability.** There is a group of concerns relating to the usability, security, trust and dependability of applications and services accessible by the mobile user, together with those same aspects - usability, security, trust and dependability - of the actual communications media and channels. One may also include in this group the security-related services, functions, and interfaces, and the security of the mobile device itself. This obviously relates to the user *trust* aspects, below in JW21, as does the necessity of security and dependability in provision of any sort of trusted service. More elaborate scenarios envisage a dynamic, heterogeneous environment delivering ambient communications and services – seamless, secure, and dependable. Meanwhile how can the same ambience be exploited to contribute to the wellbeing of the planet and its occupants. Note: fundamental to the provision of trusted emergency services is the provision of dependable access; this is currently not delivered by most cordless DECT phone systems, which are dependent on mains power for operation, unlike old-fashioned PSTN connections and the mobile phone.	1. Empowerment 5. Development processes 4. Interoperability 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security	1. Empowerment 3. Availability 5. Development processes 4. Interoperability 6. Preservation 7. User centric standardisation 8. Service-oriented architectures 9. Technologies for security
JW 20.	**Trusted device.** There is a requirement and expectation about exploiting and extending the capabilities of the mobile device to make aspects of our lives easier and more easily managed: as a generalised access control device to enable physical access, and to provide login, signature, etc.; as a universal payment token, electronic purse, and authorisation tool for higher-value transactions; and to provide storage of and access to information – local caches and secure vaults: instant facts and figures as well as critical personal and health-related data. All of this is dependent on the trustworthiness of the device itself, and of the services accessed.	5. Development processes 4. Interoperability 9. Technologies for security.	5. Development processes 3. Availability 4. Interoperability 6. Preservation 9. Technologies for security.
JW 21.	**User Trust Aspects.** Two aspect of trust are identified: subjective – dependent on personal feeling or belief, supported by, say, reputation systems and frameworks; objective – based on assurances of verifiable trustworthiness of hardware or software functionality, including cryptography, trusted computing, security protocols, etc. Some form of metrics are required on which trust-based decisions may be made. Questions arise about how trust is established, maintained,	1. Empowerment 5. Development processes 4. Interoperability	1. Empowerment 3. Availability 5. Development processes

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	monitored and reported, and how charging and payment can be made trustworthy. Considerable technology is already available; however, accompanying work is required to provide human sciences/ engineering support. The challenge is to establish a comprehensive framework for handling trusted relationships between all relevant entities, not just human users. Further investigation is required into the possible role of trusted parties as referees or brokers: how are credentials established? What are the liabilities of an entity that charges for trust-related services?	8. Service-oriented architectures	4. Interoperability 8. Service-oriented architectures
JW 22.	**Usability.** From the naïve end-user to the expert system manager, the issue of usability of security is of great importance. The provision of all sorts of procedures and technical measures is valueless if they are not to be correctly exercised, either through ignorance or wilfulness – or even necessity, if the design is actually wrong. In addition to the provision of the necessary technical interfaces, research is indicated into the design of the human interfaces and procedures, and the design and provision of contextual help and support, as well as preparatory instruction and training. The research challenge is what can users actually understand: of the interfaces and available instruction, and also of what is actually going on, and why – in particular, are critical situations recognisable to the combination of the system manager and his toolkit?	1. Empowerment 7. User centric standardisation	1. Empowerment 7. User centric standardisation
JW 23.	**Regulatory issues and legislation implications.** The need for significant research into the relevant legal and ethical issues is required for mobile computing (especially ambient intelligence, pervasive computing), an arena that is facing a serious resistance because of these issues. With the general trend of outsourcing services to external companies/countries, we need to evaluate the 'impacts of outsourcing of security functionalities' also relative to the legal framework in which the outsourcing takes place. Outsourcing is creating a new business relationship that "intervenes" with an existing one, and, thus, the issues of data protections laws are in danger of being forgotten. They are very important and, therefore, the challenge is multidimensional and not only a technological one. Moreover, policy makers need to be exposed within actual projects to economic and social risks of R&D security. Some of regulatory and legal challenges include the (i) creation of new, or the modification of existing, laws and/or regulations or (ii) identification of a new legal and regulatory body to enable sanctions and enforcement abilities for security and dependability, preferably outside of the government sphere. There is also a need for the research and business experimentation, including real users involvement and input, to be carried out and tested in the funded projects. There is a need for truly interdisciplinary FP7 RTD projects related (not just) to usability - societal and business driven, as opposed to just technical – that typically need to be of long duration; because interdisciplinary research takes quite a while to become effective as the people from different disciplines learn to work together effectively.	1. Empowerment 7. User centric standardisation	1. Empowerment 7. User centric standardisation
JW 24	**Effective and effective Certification Environment.** The elements required for an effective and economic certification environment would require an evolution of security metrics to determine the levels of security. Today, security services are either enabled or disabled and finer granularity is required. There is a need to increase certification level transparency. i.e. relate security increase to level increase and risk decrease --> economic impact of certification. Cross certification amongst different service providers e.g. via real time negotiation algorithm and dynamic certification with virtualisation for third parties based on trusted community is needed.	1. Empowerment 7. User centric standardisation 8. Service-oriented architectures	1. Empowerment 7. User centric standardisation 8. Service-oriented architectures
JW 25.	**Future Business Models.** There is a need to look at the quantified business impact of having security and dependability, highlighting the associated economic losses, so as to wake up people without unnecessarily frightening and/or discouraging them. Security should be a business enabler and not a showstopper and we should be capable of	1. Empowerment 5. Development processes	1. Empowerment 3. Availability 5. Development

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	correlating security impact with business impact in real time with advanced security analysis tools.	7. User centric standardisation 8. Service-oriented architectures	processes 6. Preservation 7. User centric standardisation 8. Service-oriented architectures
BSI 1.	**European leadership in biometric development across the authentication chain.** Europe has proven expertise in building reliable biometric systems this is rare in the current environment, there are already mature systems working in Europe. We should support the development of mature, secure and dependable systems and avoid the deployment of immature systems. Those early systems are not technically correct and propagate a negative perspective on biometrics systems. Europe demands the establishment of a European test and certification centre, in order to support European organisations (government, companies and users) in making appropriate decisions and adopting the right technology. In the short term, current FP6 projects are investigating novel biometrics and integration is taking place, three novel pilots covering wide range of applications and future use of biometrics. In the medium (2007-2010) and longer term (2010-2013), further exploitation of physiological biometrics will need to be researched including the use of even less obtrusive sensors.	1. Empowerment 2. EU-specifics 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security	1. Empowerment 2. EU-specifics 3. Availability 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security
BSI 2.	**Promote European values in the integration of identity in the network society paradigm, taking into account the European cultural space. Harmonisation of Biometrics across Europe.** A network society calls for continuous integration of applications in new areas (eGovernment, eHealth, etc…). Those applications are not probably new outside the European geographical space, but Europe should integrate them in a respectful framework. It will lead Europe towards the excellence and the reference in the deployment of network services. An important step towards this challenge is the scenario development, where pilot systems are designed, integrated, built and studied in a controlled, adaptive and evolving environment, with the opportunity to become "research testbeds" for the adoption of biometrics in every day scenarios (private spaces, electronic signature, network applications). This would enable the gathering of real data on the impact of the deployment of biometrics at the socio-economical level. Another important feature of the deployment of biometrics is embedding data protection into technology deployments and architectures through development of specifications, protocols and tools to keep the required level of assurance and certification. By means of new tools, organizations and users may evaluate the compliance of systems towards legal, security and dependability risks and conformance. In the short term, in current FP6 projects, the BIOSEC biometrics API are bring used, standardization, contribution to the relevant biometrics standards are being undertaken and three novel pilots covering wide range of applications and future use of biometrics. In the medium (2007-2010) and longer term (2010-2013), there is a need to address the creation of new standards and modification of the existing ones in order to cover the use of new biometrics modalities that will result from IST project HUMABIO R&D, including standardization of authentication procedures/protocols.	1. Empowerment 2. EU-specifics 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security	1. Empowerment 2. EU-specifics 3. Availability 5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security
BSI 3.	**Leading Europe towards developing cutting-edge technology.** This would include novel pattern recognition approaches that would support the integration of biometrics in the ICT systems of the future. In addition, testing procedures and tools, towards security certification and/or evaluation of biometrics systems (databases, testing	1. Empowerment 2. EU-specifics 5. Development	1. Empowerment 2. EU-specifics 3. Availability

Challenge reference	STF Challenge	Advisory Board Recommendations	
		Medium term	Long term
	protocols and procedures, compliance tools). Multimodal biometrics is the key for massive deployments of biometrics, but several issues are in the agenda of researchers: testing and supporting tools, efficient algorithms, guide to choose suitable combination of biometrics according to applications, etc. Europe is already leading the research in Aliveness detection, but an important support is required to keep the path. Those features will support the development of identity providers in the network society. In the short term, EEG, ECG, ERP biometrics will be studied and utilized in working prototypes for the first time. Use of novel unobtrusive sensors for physiological measurements applied in biometrics for the first time. Work will be carried out on token based systems (ePass, ECC), biometric template protection (compact coding), robustness against system noise to allow hashing and application in 1-to-1 comparison scenarios. In the medium (2007-2010) and longer term (2010-2013), further miniaturization of the biometrics sensors, complete unobtrusiveness for the subject, integration of the biometrics system with the ambient intelligence infrastructure, transparent and continuous operation of the system will need to be addressed. Future work will need to be done on DB based systems (Visa information systems, industrial environments), renewability and revocability of stored templates, application in 1-to-n comparison scenarios, automated self-identification, ICAO's perspective: unattended border crossing, exploitation of the three-dimensional acquisition space and proof fake resistance.	processes 4. Interoperability 7. User centric standardisation 9. Technologies for security	5. Development processes 4. Interoperability 7. User centric standardisation 9. Technologies for security

10 Annex V – Other Related Initiatives

Table of Contents

This Annex provides details of existing related and relevant initiatives within the European Union and the United States relating to ICT Trust, Security and Dependability.

10.1 Related European Initiatives

10.1.1 European Union Communication on CIP

The Communication of the Commission of the European Communities (EU Commission) on "Critical Infrastructure Protection in the Fight Against Terrorism", adopted on 20 October 2004, provides a definition of critical infrastructures (CI), enumerates the critical sectors identified, and discusses the criteria for determining potential CI. In the Communication, CI is defined as follows: "Critical infrastructures consist of those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments in the Member States. Critical infrastructures extend across many sectors of the economy and key government services."

In the follow-up publication of the EU Commission, the "Green Paper on a European Program for Critical Infrastructure Protection" (Green Paper on EPCIP), CIIP is defined as: "The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of CII in case of failures, attacks or accidents above a defined minimum level of services and aim at minimizing the recovery and damage. CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with CIP from a holistic perspective."

10.1.2 Critical Information Infrastructure Research Co-ordination (CI2RCO)

The EU has set up a task force to explore the measures taken by its 25 member states to combat (cyber-) threats against critical infrastructure. As part of the EU's CI2RCO (Critical Information Infrastructure Research Coordination) project, announced in April 2005, the task force aims to identify research groups and programs focusing on IT security in critical infrastructures, such as telecommunications networks and power grids. The scope of the cooperation goes beyond the EU; the task force also wants to include the US, Canada, Australia, and Russia. The CI2RCO project is a Co-ordination Action co-funded under the IST FP6. The main objectives of the CI2RCO project are:

- Encouraging a coordinated Europe-wide approach for research and development on CIIP;

- Establishing a European Research Area (ERA) on CIIP as part of the larger IST strategic objective of integrating and strengthening the ERA in terms of dependability and security.

CI2RCO will focus on activities and actions across the EU-25 and Associate Candidate Countries. Among other information, the CI2RCO website features the "European CIIP Newsletter" and upcoming events in the area of CIIP.

10.1.3 European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) was created on 14 March 2004. By deciding on 5 June 2003 to set up ENISA as a legal entity, the EU reinforced its efforts to enhance European coordination on information security.

ENISA aims at ensuring a high level of network and information security within the community. Thus, the agency will contribute to the development of network and information security for the benefit of the citizens, consumers, enterprises and public sector organizations of the EU. This will also contribute to the smooth functioning of the Internal Market.

The agency assists the EU Commission, the member states and, consequently, the business community in meeting the requirements of network and information security, including present and future EU legislation. ENISA will ultimately serve as a centre of expertise both for member states and for EU institutions to seek advice on matters related to network and information security.

The work program for 2005 included several deliverables. The European Network and Information Security Agency (ENISA) has created a "Who is Who Directory on Network and Information Security" with contact information for authorities acting in the field of network and information security in the member states. ENISA has also published an "Inventory of CERT Activities in Europe" and issues a quarterly newsletter. In addition, ENISA organizes workshops for outreach and dissemination of good practices in the member states. Moreover, ENISA will define customized information packages, including good practices for specific target groups (e.g. SMEs and home users). Finally, ENISA has created a network of liaison officers, which helps ENISA to exchange information and cooperate on a day-to-day basis with member states.

In line with its work program for 2005, ENISA has set up the Permanent Stakeholders' Group (PSG). It brings together experts from the industry, academia, and user communities, and has become an invaluable tool for ENISA's cooperation with these communities. Moreover, three working groups have been established in the fields of CERT cooperation, awareness-raising, and technical and policy aspects of risk assessment and risk management.

10.1.4 European Security Research Programme (ESRP)

The goal of European security research is to make Europe more secure for its citizens while increasing its industrial competitiveness. By co-operating and coordinating efforts on a Europe-wide scale, the EU can better understand and respond to risks in a constantly changing world. For projects in the field of security research, the following priority missions are identified:

- Optimizing the security and protection of networked systems;

- Protecting CI against terrorism (including bio-terrorism and incidents involving biological, chemical, and other substances);

- Enhancing crisis management (including evacuation, search and rescue operations, control, and remediation);

- Achieving interoperability and integration of systems for information and communication;

- Improving situation awareness (e.g. in crisis management, anti-terrorism activities, or border control). 832

Furthermore, the EU Commission set up the European Security Research Advisory Board (ESRAB) on 1 July 2005. The ESRAB is attached to the EU Commission and can be consulted on any questions related to the content and implementation of the European Security Research Program. ESRAB carries out its work in full awareness of the European policy context, in particular of the research and development activities carried out at the national level and in support of European research policy initiatives.

10.1.5 Council Framework Decision on Attacks against Information Systems (2005)

The European Council Framework Decision on attacks against information systems (2005/222/JHA) 847 of February 2005 aims to strengthen criminal judicial cooperation on attacks against information systems by developing effective tools and procedures. The criminal offences punishable under the framework decision are: illegal access to information systems, illegal system interference (the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, degrading, altering, suppressing, or rendering inaccessible computer data) and illegal data interference. The member states will have to make provisions for such offences to be punished by effective, proportionate, and dissuasive criminal penalties. To enhance cooperation, the member states must establish operational points of contact that are available 24 hours a day and seven days a week.

10.1.6 Directive on Data Retention (2005)

In December 2005, the European Parliament agreed on a Directive on the Retention of Data processed in connection with the provision of public electronic communication services (Commission proposal COM(2005)0438). This legislation, which allows the individual governments to decide how long data should be retained as long as the period is between six and 24 months, is likely to take effect during 2006, although it may face legal challenges in several countries. The measures, drafted by the United Kingdom after the London terrorist bombings in July 2005, require companies to keep a wide range of data, including incoming and outgoing phone numbers; the duration of phone calls; data that can be used to trace fixed or mobile telephone calls; information about text messages; IP addresses, which identify a computer's coordinates on the internet; login and logoff times; and details of e-mail traffic – but not the actual content of communications. Details of connected calls that are unanswered, which can be used to send signals to accomplices or to detonate bombs, will also be archived where that data exists. Independent authorities will be designated to monitor the use of the data, which will have to be deleted at the end of the period unless it is kept for anti-terror investigation purposes.

10.2 United States

Critical Infrastructure Protection (CIP) in the US refers to the protection of infrastructure critical to the people, economy, essential government services, and national security. The main goal of the US government's efforts is to ensure that any disruption of the services provided by this infrastructure is infrequent, of minimal duration, and manageable.

There have been several efforts since the 1990s to better manage Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) in the US. CIIP plays an important role in the overall US security strategy. The US government views CIIP as an element of its homeland security strategy. Where traditionally, national security has been recognized as the responsibility of the federal government and is underpinned by the collective efforts of the military, the foreign policy establishment, and the intelligence community with respect to defence, homeland security is viewed as a shared responsibility that requires coordinated action across many sectors.

The US government is especially committed to CIIP, as evidenced by President George Bush signing a US$37.4 billion Homeland Security appropriations bill for 2004. US$839.3 million was allocated specifically to the Information Analysis and Infrastructure Protection Directorate, which has responsibility for cyber-security as well as for the telecommunications and IT sector. Among other measures, this money will fund research and development in examining network weaknesses and evaluating threats and vulnerabilities.

10.2.1 National Plan for Information Systems Protection

On 7 January 2000, President William Clinton presented the first comprehensive national plan for CIIP — focusing on securing the cyber-components of critical infrastructures, but not the physical components – called "Defending America's Cyberspace. National Plan for Information Systems Protection – An Invitation to Dialogue Version 1.0". This plan reinforced the perception of cyber-security as a responsibility shared between the government and the private sector.

10.2.2 National Strategy to Secure Cyberspace

The "National Strategy to Secure Cyberspace (NSSC)" recognizes that securing cyberspace is an extraordinary challenge that requires a coordinated effort from all parts of society and government. In order to achieve this goal and to engage the public in securing cyberspace, a draft version of the NSSC was initially released for public comment, and ten town hall meetings were held around the US to gather input on its development. This careful vetting process is a clear sign that cyberspace security is viewed as an issue that requires a public-private partnership, since the government neither owns nor operates most of the cyber-infrastructure.

The NSSC defines cyberspace as an "interdependent network of information technology infrastructures" and depicts cyberspace as the nervous system or control system of society. The NSSC outlines an initial framework for both organizing and prioritizing national efforts in combating cyber-attacks committed by terrorists, criminals, or nation-states, while highlighting the role of public-private engagement.

Consistent with the National Strategy for Homeland Security, the strategic objectives of the NSSC are:

- To prevent cyber-attacks against the national CI;
- To reduce the national vulnerability to cyber-attacks;
- To minimize damage and recovery time from cyber-attacks.

The strategy recognizes that, as owners and operators of much of the internet infrastructure, the private sector is best equipped and structured to respond to cyber-threats. Therefore, public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

10.2.3 DHS/Directorate for Information Analysis and Infrastructure Protection (IAIP)

As one of the five major divisions of the US Department of Homeland Security, the Directorate for Information Analysis and Infrastructure Protection (IAIP) is responsible for identifying and assessing current and future threats and vulnerabilities to the homeland, issuing timely warnings, and taking preventive and protective action. The directorate focuses special attention on the protection of critical infrastructure and cyber-security.

The IAIP leads and coordinates the national effort to secure the nation's infrastructure and fosters an active partnership with the private sector. In creating the IAIP, the government's goal was to establish a central contact point for state, local, and private entities to coordinate protection activities with the federal government.

The IAIP has unified and focused the key cyber-security activities of the Critical Infrastructure Assurance Office (CIAO), formerly part of the Department of Commerce; the National Infrastructure Protection Center (NIPC), formerly a subdivision of the FBI; and the Federal Computer Incident Response Center (FedCIRC), formerly of the General Service

Administration. Because CI relies heavily on information and telecommunication services and interconnections, the IAIP also assumed the functions and assets of the National Communications Systems of the Department of Defense, which coordinates emergency preparedness for the telecommunications sector and some responsibilities of the Energy Security and Assurance Program of the Department of Energy.

The IAIP directorate currently consists of four divisions. These include the Infrastructure Coordination Division (ICD), the National Cyber Security Division (NCSD), the Protective Services Division (PSD), and the National Communications System (NCS).

10.2.4 Computer Crime and Intellectual Property Section (CCIPS)

The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the Department of Justice is responsible for implementing the department's national strategies in combating computer and intellectual property crimes worldwide. The Computer Crime Initiative is a comprehensive program designed to combat electronic penetrations, data theft, and cyber attacks on critical information systems. CCIPS prevents, investigates, and prosecutes computer crimes by working with other government agencies, the private sector, academic institutions, and foreign counterparts.

10.2.5 Information Sharing and Analysis Centers (ISACs)

Today, most critical infrastructure industry sectors have established their own Information Sharing and Analysis Center (ISAC). Private-sector ISACs are membership organizations managed by the private sector. Each ISAC has a board of directors that determines its institutional and working procedures. The function of an ISAC is to collect, analyze, and share security, incident, and response information among ISAC members and with other ISACs, and to facilitate information exchange between the government and the private sector. The following list gives an overview of important existing ISACs:

- A number of the nation's largest banks, security. rms, insurance companies, and investment companies have joined in a limited liability corporation to form a Financial Services Information Sharing and Analysis Center (FS/ISAC).

- The telecommunications industry has established an ISAC through the National Coordinating Center (NCC). Each member. rm of the NCC monitors and analyzes its own networks. Incidents are discussed within the NCC, and members decide whether the suspect behaviour is serious enough to report to the appropriate federal authorities.

- The electric power sector has created a decentralized ISAC through its North American Electricity Reliability Council (NERC). Much like the NCC, the NERC already monitors and coordinates responses to disruptions in the nation's supply of electricity. The government and industry work together in the NERC to ensure the resiliency of the electricity infrastructure in case of potential physical and cyberspace attacks.

- The IT-ISAC started operations in March 2001. Members include 20 major hardware, software, and e-commerce firms, including Cisco Systems, Microsoft, Intel, Computer Associates, Symantec, Computer Sciences Corporation, and Oracle. The ISAC is overseen by a board made up of members, and its operations centre is managed by Internet Security Systems.

- Other ISACs include the Surface Transportation ISAC, the Oil and Gas ISAC, the Water Supply ISAC, the Chemicals Industry ISAC, the Emergency Fire Services ISAC, the Emergency Law Enforcement ISAC, the Food ISAC, the Health ISAC, and the Multi-State ISAC.

• In addition to the individual sector ISACs, several ISAC leaders have convened as an ISAC Council. This council strives to strengthen the relationship between the ISAC community and government, and to solve problems common to all ISACs.

10.2.6 InfraGard

InfraGard is a partnership between industry and the US government as represented by the FBI. The InfraGard initiative was developed to encourage the exchange of information by members of the government and the private sector. With help from the FBI, private-sector members and FBI field representatives form local chapter areas. These chapters set up their own boards to share information among their membership. This information is then disseminated through the InfraGard network and analyzed by the FBI.

10.2.7 National Cyber Security Alliance (NCSA)

The National Cyber Security Alliance (NCSA) is a cooperative effort between industry and government organizations to foster awareness of cyber-security through educational outreach and public awareness. Its goal is to raise citizens' awareness of the critical role that computer security plays in protecting the nation's internet infrastructure, and to encourage computer users to protect their home and small-business systems. It offers computer security advice and tools for private users as well as small businesses on its website. The NCSA is sponsored by a variety of organizations.

10.2.8 Cyber Incident Detection & Data Analysis Center (CIDDAC)

The Cyber Incident Detection & Data Analysis Center (CIDDAC) is the first private, non-profit group to set up a cyber-crime detection network outside of the US government's own efforts. The purpose of CIDDAC is to manage an automated reporting infrastructure for cyber-attacks that supports the protection of the national infrastructure. CIDDAC combines private, public, and government perspectives to facilitate automated real-time sharing of cyberattack data. Thirty undisclosed organizations are working with CIDDAC on its pilot scheme. Each will be provided with CIDDAC's Remote Cyber Attack Detection Sensor, which will feed intrusion data into the CIDDAC center, where it can be evaluated and passed on the law enforcement agencies.

10.2.9 National Cyber Security Partnership (NCSP)

The National Cyber Security Partnership (NCSP) is a voluntary coalition of industry trade associations committed to working on cross-sector cyber-security issues in a collaborative manner. NCSP members include representatives of software makers, hardware manufacturers, and the end-user community, including colleges and universities. NCSP founding members include the US Chamber of Commerce, TechNet, the Business Software Alliance, and the Information Technology Association of America (ITAA).

Following the release of the 2003 White House National Strategy to Secure Cyberspace, the NCSP sponsored the National Cyber Security Summit to develop shared strategies and programs to better secure and enhance the US critical information infrastructure. The partnership established five task forces of cyber-security experts from industry, academia, and the government.

10.2.10 Institute for Information Infrastructure Protection (I3P)

The Institute for Information Infrastructure Protection (I3P), managed by Dartmouth College, is a consortium of leading national cyber-security institutions, including academic research centres, government laboratories, and non-profit organizations. Founded in September 2001, the institute's main role is to coordinate a national cyber-security research and development program and to help build bridges between academia, industry, and the government. The I3P identifies and addresses critical research problems in CIIP and opens information channels between researchers, policy-makers, and infrastructure operators.

10.2.11 Early Warning and Public Outreach

Information-sharing is one of the driving factors behind effective early-warning networks. Many entities focused on information-sharing are also engaged in early-warning activities.

11 Annex VI – SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework

Information Society and Media

SecurIST

SecurIST Advisory Board

Recommendations for a Security and Dependability Research Framework:

from Security and Dependability by Central Command and Control to Security and Dependability by Empowerment

Issue 3.0
15 January 2007

Project no. 004547

Project acronym: SecurIST

Project title: Co-ordinating the development of a Strategic Research Agenda for Security and Dependability R&D *(Steering Committee for a European Security & Dependability Taskforce)*

Instrument: Coordinating Action

Priority: SIXTH FRAMEWORK PROGRAMME
PRIORITY 2
Information Society Technologies

SecurIST Advisory Board Recommendations for a Security and Dependability Research Framework

From “Security and Dependability by Central Command and Control”
to “Security and Dependability by Empowerment”

Issue 3.0

15 January, 2007

Project co-funded by the European Commission within the Sixth Framework Programme (2002-2006)		
Dissemination Level		
Public	Public for interested parties involved in preparation of Work Programme for FP7.	

Part I - SecurIST Advisory Board Recommendations

Table of Contents

Management Summary

The SecurIST Advisory Board has undertaken the task of examining the requirements for the European Security and Dependability Research Framework from the perspectives of the Information Society's various stakeholders, with a particular focus on those of the individual or citizen within this Society. The information systems that make up the European Information Society in this context consists of hardware, software, processes and people, thus covering non-technical as well as technical aspects. Stakeholders of the Information Society include (but are not limited to) individual citizens, SMEs, large corporations, non-governmental organisations and governments, and indeed the research community itself.

The Advisory Board believe that it is important to address all the different facets of security and dependability in the European Information Society. Dependability is an integrating concept that encompasses the qualities or attributes such as availability, reliability, safety, integrity, and maintainability, and mainly seeks to achieve these attributes in the face of possible accidental physical and design faults. Security is seen as encompassing the confidentiality[17], integrity and availability of information and seeks to preserve these properties in the face of any threat that may compromise them such as software failure, human error or deliberate attack. The two concepts, overlap extensively, and are closely inter-related. In order to get the maximum benefits of research results going forward, an interdisciplinary and integrated approach is required which goes beyond focussing on narrow technological issues.

The SecurIST approach is complementary to the approach by the European Security Research Advisory Board ESRAB [1], which is rather focused on security from a government and enterprise perspective and to the work of the European Network and Information Security Agency ENISA [2], focussing on best practices in Computer Emergency Response Team (CERT) co-operation, risk management and awareness.

There are many stakeholders in the European Information Society and it is important to look at problems, needs and solutions from the perspective of them all. However, the problems and needs of individuals deserve a particular focus. End-users, in particular individual citizens are, understandably, becoming more and more concerned about the increasing complexity of information systems, about the trend toward central control and monitoring in electronic environments and about the continued attempts to make every digitized action accountable by associating it with identities that lead back to individual citizens, corporate entities or members of organisations. To keep up to date with the increasing rate of change of the information society, the end-users find themselves having to put ever more trust into environments they have no way of understanding or assessing. In other words, the risk of using the Information Society's processes and systems appears to be increasing: risks such as identity theft and abuse; disclosure of sensitive information; wrong attribution of charges – *financial* or *criminal*. Currently, such issues are evolving trends only, so for a secure and dependable Europe there are challenges but there are also opportunities. Focused correctly, research for a secure and dependable Information Society can lead the way towards a future environment in which the risks to the various end-users, in particular to individual citizens, of living in the Information Society are significantly lower than they are today.

The Advisory Board has come to the conclusion that given these trends, if there is to be a secure and dependable future Information Society in Europe, the following nine key areas need to be addressed in a European Security and Dependability Research Framework: These are outlined on the following page. In addition to these nine key areas, four future *grand challenges* are given that illustrate possible longer-term possibilities and implications. While offering new freedoms and opportunities, they also present new and dangerous security and dependability risks to the individual and to society, and set new challenges to the research community.

The Board's report, recommendations and review of requirements, is contained in Part 1 of the document; Part 2 contains an extensive glossary and informative annexes.

[17] including privacy aspects

Key areas for a European Security and Dependability Research Framework

1. Empowerment of the various types of Stakeholder, and in particular of Citizens:
Empowerment of the citizen [3] is vital as there is a clear technological trend towards the decentralization of technology and its management and control. Current centralized control structures need to be enhanced or perhaps even replaced, since security and risk management considerations, e.g. concerning identity theft, in fact imply that responsibility, authority and control have to move more towards the end user. If the user is to be accountable, then the user must have proper protection and control.

2. Europe-specific Security and Dependability:
Europe has a very particular yet heterogeneous culture, history, and set of attitudes to trust and society. The European Information Society will have the possibility to compete successfully with information societies being established in other regions of the globe if and only if Europe-specific needs are taken into account and actively addressed by technological and socio-technical research projects in a structured manner.

3. Infrastructure Robustness and Availability:
As stakeholders come increasingly to rely on ICT infrastructure, covering both local infrastructure such as software, and hardware devices, and network infrastructure, involving various communications technologies, the assurance of the robustness and availability of the infrastructure grows in importance. Over and beyond ICT infrastructure, there is an evident requirement for reliable and available critical infrastructures such as medical, energy, telecommunications, transport, finance, administration and emergency services.

4. Interoperability:
The future is unlikely to be a homogeneous, standardized technology for communications purposes, but rather a whole range of fixed and mobile communications technologies, ranging from body area networks to broadband broadcast communications across national borders. If this complex web of technologies is to function effectively, it is crucial that there will be semantic interoperability between security and dependability technologies.

5. Processes for developing more secure and dependable systems:
There needs to be systematic improvement of methods of developing secure and dependable systems, including hardware and software, right from the beginning of the development process, whether one is constructing an entirely new system, or one composed of pre-existing systems.

6. Security and Dependability Preservation:
Once systems have been developed and installed, the maintenance of effective system security and dependability is critical. This is particularly true in an increasingly complex world of evolving requirements, technologies and systems. Preserving security and dependability also means preserving the confidence users have with regard to information privacy, transaction correctness, etc.

7. User-centric security and dependability standardization:
Strengthening of the structured involvement of end-users, in particular citizens and their respective representatives or institutions, into all relevant security and dependability standardization activities.

8. Security and Dependability of Service Oriented Architectures (SOAs):
Means are needed to establish and maintain trust and to manage policy regulations and Service Level Agreements regarding security and dependability, in an SOA context, together with commensurate advances in software engineering to deliver service expectations.

9. Technologies for security:
Underlying all of these is the need to provide higher assurance of trusted communication and handling of digital information. The two fundamental sciences and technologies are (a) cryptology and (b) trusted functionality and computing. Cryptology ensures the protection of information stored or in transit outside a trusted area. The trusted functionality creates and maintains that trusted area, and ensures that information is handled within it as intended, and that the cryptographic processes are correctly executed. Security protocols establish and maintain trusted communication between trusted areas. Both disciplines need sustained R&D to keep ahead of the needs of their dependants.

Introduction

This Report is structured into four chapters. Chapter one represents the rationale and introduction, highlighting the security and dependability situation in the first decade of the 21st century. Chapter two discusses security and dependability requirements of the European Information Society's citizens and what is involved in providing these requirements. Chapter three explains the key recommendations in detail. A fourth chapter presents possible future challenges that illustrate the need to be already prepared for new scientific and technological developments and directions. A list of references, an extensive glossary, and informative annexes complete the Report.

The SecurIST Advisory Board

The SecurIST Advisory Board [Annex I] is composed of European experts in Information Security and Dependability and has the task of reviewing results from the Security and Dependability Task Force. The Advisory Board has met physically a number of times, and were presented with the challenges identified by the different Task Force Initiatives and the rationale behind the challenges. The Advisory Board has prepared documentation and given presentations on its preliminary findings [4]. The Board also has established and will continue establishing links to other relevant European activities and bodies that are of relevance to security in the future European Information Society, such as the European Security Research Advisory Board ESRAB, and the European Network and Information Security Agency ENISA.

The SecurIST Advisory Board members' personal reputation and competence, their extensive experience and their well-established contact networks in Information Security have been used to build and promote a consolidated picture particularly, but not solely from a citizen's perspective, of the future Information Society. This is the subject of the present report.

Security and Dependability in the first Decade of the 21st Century

Security and dependability have been continuously among the key issues on the list of the European Council's presidencies and will remain a major challenge to Europe and to the global community for the upcoming years. Terrorist attacks have become a global threat and society becomes more and more dependent on critical infrastructures of ever greater (indeed in many cases unmastered) complexity. Therefore, security and dependability research must be focused on the right topics and a research agenda must take into account different facets of the broad subject area of "security and dependability". These facets include physical security, electronic security, critical infrastructure protection and IT security, in the face of deliberate attacks, and both system and infrastructure dependability and indeed security, in the face of physical malfunctions and residual design defects.

Dependability is an integrating concept that encompasses the following attributes: availability, reliability, safety, integrity, and maintainability, and mainly seeks to achieve these attributes in the face of possible accidental physical and design faults. Security is a concept encompassing the confidentiality, integrity and availability of information and seeks to preserve these properties in the face of any threat that may compromise them such as software failure, human error or deliberate attack. The two concepts thus overlap somewhat, and are closely inter-related. Successful security breaches commonly are based on exploiting vulnerabilities that exist as a result of residual system design faults or during periods of physical failures, and dependability can be badly affected as a result of unauthorised actions that were not prevented by appropriate security mechanisms. In what follows, therefore, the phrase "security and dependability" occurs frequently – a possible abbreviation for this phrase is "trustworthiness" [5]. However, effective security and dependability research will need to broaden its scope from purely technological aspects and to address related areas with equal emphasis, e.g.:

- Interdisciplinary approaches
- Socio-technical research,
- Industry trends (e.g. such as outsourcing and offshoring)
- Co-ordination between policy makers and technical research.

The evolution of our digital society is characterized by ubiquitous computations, communications and storage, and by the development of services that are personalized and context-aware. In the coming years, we will notably see the deployment or emergence of new information and communication infrastructures like converged mobile and fixed networks based on the IMS architecture, WiMAX networks, corporate networks with Voice over IP or multimedia, Peer to Peer structures, networks of sensors/actuators with scarce data-processing resources or the *Internet of Things* [6].

The trend is towards the emergence and deployment of ever more massively distributed, interoperable and interdependent complex ICT systems composed of billions of interacting components whether fixed or mobile. Their emergence will create new, unprecedented challenges for Security, Dependability and Trust as for example: security and dependability of Beyond-3G infrastructures and the new cellular networks (security of mobility, services and their supervision); trust, security and dependability of post-IP networks, in particular the Future Internet, also in relation to international work in this area (NSF initiatives FIND, GENI) and trust, security and dependability attributes in the architecture and design of future networked systems, as for example new protocols, adaptive detection, diagnosis, and run-time response mechanisms and stochastic security in core/access networks from an end-to-end perspective; the protection of critical infrastructures and their interdependencies; security and dependability of software systems and services including security and dependability of overlay networks, overlay services (dynamic virtual systems), security of the virtualisation paradigm (horizontal and vertical hand-overs and associated security, nomadic fast authentications, services in real time, massively distributed, multi-users, management of these services.

At the smallest level, nanotechnology, quantum communication and cryptography offer new opportunities to tackle ICT security. Embedded sensors and devices can form ad-hoc networks requiring new mechanisms for establishing trust when sharing information or resources. New paradigms come to the foreground, such as service architectures that compose services from lower level modules, peer-to-peer systems characterized by their remarkable robustness and resilience against attack, and biological defence mechanisms, which may inspire new breakthrough technologies. At a larger scale, the completion of the Galileo satellite navigation system around 2009 will create ever more sophisticated possibilities for positioning with implications for both security and privacy.

Against this background, this document presents the view of the SecurIST Advisory Board on the security and dependability challenges and requirements for the Information Society in Europe. It is based on the work of the board members during 2005 and 2006, as well as on several meetings/workshops and it takes into account the findings and challenges listed in the report from the Security and Dependability Task Force [7]. The document is meant to complement the preliminary findings of the European Security Research Advisory Board ESRAB and work of the European Network and Information Security Agency ENISA, by adding the European Information Society citizens' perspective on security and dependability.

Globalisation

Globalisation is already having a major impact on all the countries in Europe, and the role of the European Union is therefore two-fold, aiming at internal and external goals: the future European Information Society will have to create interconnectivity and harmonisation between the European Member States and will also have to find its role in the global environment with American and Asian markets that are competitors and partners at the same time.

Information is already considered a valuable commodity, but present and future information networks do not end at national borders nor is there any strong separation between the United States, Europe and Asia. Physical infrastructures are merging and converging; virtual networks, ubiquitous computing and ambient networks have started to replace today's concepts of central network control. The same interdependency that is visible in communications infrastructures is partly also occurring for other critical infrastructure sectors such as power and energy supply, transport and financial services. The effects of faults, whether accidental or deliberate in origin, can if not adequately controlled, cascade from one system to another, and have catastrophic effects on the reliability, availability and security of these systems. The challenge for the future European Information Society, therefore, is neither limited to the geographical area of Member States nor can it be addressed by European regulations alone.
A balance must be maintained between playing a fully participating role in the global enterprise and the need to avoid domination and control of our essential infrastructures by non-European interests.

Furthermore, the competitive situation, especially towards a highly advanced IT and security technology market in Northern America and a low-cost high-speed development in South-East Asia, forces Europe to find its own position with respect to security and dependability in general and IT security and dependability specifically. The very strengths developed by Europe in the area of security and dependability provides a significant opportunity for their exploitation, and the provision of solutions worldwide.

European Activities

In a European environment, security and dependability are discussed in various contexts, including areas such as

The role of Europe in the world-wide fight against terrorism,

European border control across now 27 member states,

IT security activities as addressed e.g. by the European Network and Information Security Agency ENISA,

A dedicated European Security Research Programme ESRP as part of the 7th Framework Programme,

Protection of the future European Information Society with special attention to the Information Society citizens' requirements,

The robustness of the Information Society's systems and infrastructures on which citizens are expected to place ever greater dependence and trust.

The Information Society Stakeholders

The Stakeholders

The European Information Society has a range of stakeholders, including SMEs, large corporations, government departments, non-governmental organisations and individuals in the role of employee, consumer, shareholder and citizen. Each category of stakeholder has a number of problems and issues facing them regarding security and dependability.

The information and communication systems of large corporations are often complex systems working across many countries and used by thousands of employees. Many external parties, such as, suppliers and customers, also access these systems. In attempting to achieve systems that are secure and dependable, large corporations have to balance the risks they face from threats to their systems against the cost of security and dependability measures. Although they have specialist staff to design and develop their systems and to advise on security and dependability issues, they often face problems. What are the risks? Is there good data on threats and their likelihood? What is best practice in dealing with this new technology? What vulnerabilities will this new piece of technology introduce? What legislation and regulations affect this system? What controls will regulators demand? How much should be spent on protective measures? And these problems often have to be addressed in a difficult and competitive economic environment.

National and European governmental organisations share many of the problems of large corporations in terms of security and dependability. They often have large, complex systems, huge databases and thousands of people needing access. In building and operating their systems, government departments face the same problems regarding risks, availability of sound data, best practice and so on.

SMEs have the problem that they are too small to have several different experts on their staff to address the full range of security and dependability issues. Ideally, they would like to buy secure and dependable components that they can join together into a secure and dependable system. In essence, they need 'plug and play' security and dependability. Today, this is not really available.

Individuals also face problems regarding security and dependability, which vary depending on their particular role, such as employee or citizen. Although individuals understand security and dependability regarding physical items, such as their house, they do not have a clear understanding when it comes to their digital presence. Information and Communication systems are becoming increasingly complex and individuals are having to trust systems they do not really understand and are not fully aware of the risks involved.

The university and research institution networks have many of the characteristics of the large commercial and administrative organisations. They have an important role as both researchers and educators, but they also must also ensure that malware – perhaps generated by students out of a misplaced sense of playfulness or power – is captured, and not allowed propagate.

The problems that all stakeholders face will increase markedly as the development of the European Information Society gathers pace. In the digital world of tomorrow:

The number of devices connected to the Internet will grow by an order of magnitude,

New technology, such as GRID and RFID will become commonplace,

Computer and Communications technology will have converged and will be considered as a utility like electricity,

Access to the Computer and Communications utility will be from anywhere at any time, with seamless hand-over from fixed to wireless, and from personal networks – body, home, car – to local networks to mobile networks to an employers network.

In this environment, it is clear that the security and dependability challenges will become significantly greater and any research agenda must address the problems and issues faced by all stakeholders in the European Information Society.

However, if the above developments are inspected more closely, a number of trends can be identified:

- There is a decentralisation of technology, which implies a decentralisation of control. Many devices will communicate with other devices and this has to be under direct or indirect owner control.
- In a digital world, the importance of identity becomes critical and the management of identity by the various types of stakeholder, and in particular by individual citizens, takes on added importance.
- As the digital world begins to affect almost all facets of an individual's life, there will be greater concern about security, dependability and privacy.
- Since data is a critical resource of the information society, ensuring the control of data is in the hands of end-customers is critical to ensure that applications and services offered by value chains will align according to human needs.

The Advisory Board, therefore, believe that the needs and concerns of the individual citizen will have a profound effect on the development of the European Information Society and that particular attention should be paid to these needs.

However, it must be stressed that the solutions that emerge from research into the citizen's needs will also have a beneficial impact on the needs of all the other types of stakeholder. All large information systems involve both ICT and people. Even with dependable ICT, people are still a weak point and a prime source of security and dependability problems, e.g. through uninformed actions, or through deliberate misconduct. Thus strengthening client-side security and dependability is vital for progress:

- All value chains end in personal consumption – by focussing on client-side security and dependability, we ensure that value chains align according to customer needs and preferences as the main driver for growth. For example, organisational or server-side database security depends on user security. If you can successfully steal the identity of a security-cleared operator, you can always break into an ICT system.
- Perimeter security is failing- we have to move to security paradigms based on Security by Design.
- Citizen security is a precondition for democracy.
- We need balanced security and dependability – otherwise one citizen's protection turns into a threat to other citizens.

As the digital world begins to affect almost all facets of each individual's life, there will be greater concern about security, dependability and privacy. What is key to the position of the Advisory Board is that all security and dependability is integrated – to secure ICT we both should and need to include Citizen self-protection, as ICT security and dependability cannot be better than Citizen security and dependability. We need alignment and holistic approaches to security, dependability and privacy.

The Citizen's Perspectives on Security and Dependability

The SecurIST Advisory Board has aimed to provide a particular perspective on security and dependability from the standpoint of the citizen of the Information Society. The citizens' perspectives are, in the Board's view, characterized by the following attitudes that are unique to citizens:

Citizens will not use systems and services unless they are forced to, or can see that it is in their best interest to do so - this latter will not be the case unless they have reason to believe that the systems and services are performing correctly and efficiently, and are useful, usable and understandable. Purely technical solutions that do not take into account personal preferences, and human capacities and frailties are unlikely to be sufficient.

Citizens place a high valuation on their individual personal data:
In a company and government environment, protection of employee and company/government data is mostly enforced by policies and organization specific rules. In contrast, the genuine citizens' perspective does not consider company data or third party data but is focused on the protection and privacy of personal data and identities related to the individual citizens as end-users.

Citizens increasingly distrust ICT services and infrastructure:

- The citizen's experience in many cases is dominated by publicity about computer failures, huge unsuccessful system development projects, malware (e.g., viruses) and spam mail. In contrast to sharply focused company environments that are only accessible to an exactly specified set of employees, one has to assume that, due to the negative publicity, the average citizen will place only very limited trust into public ICT services, systems or infrastructure. In the area of dependability, the typical citizens might by now have developed at least a reasonable expectation about a service's availability. In the area of security, no such pre-existing trust concerning system integrity and preservation of privacy and confidentiality can presently be assumed.

Citizens are not well-informed regarding security nor can they easily obtain professional support and advice about security issues.
In a corporate environment or in a government environment, security rules become part of a working contract and are communicated to employees in a structured way. There are usually a comparatively small number of ICT users that are to be addressed and the possibilities to enforce security policies are manifold. The situation of the ordinary citizen is completely different. Although there are a number of relatively well-informed citizens (e.g., cautious people, experts or (self-) trained people), the majority of the citizens cannot be expected to have received special training on security or technology issues. In contrast to a corporate or administrative environment, the citizen usually has no easy access to expert consulting, helpdesk functions or professional advice in security issues either, and often there is a very poor balance between security and usability.

The citizen does not assume any responsibility for security and dependability beyond the personal environment.
From a national government perspective, there is an obligation to assure a Member State’s security and dependability and to protect critical infrastructures. The same obligation, limited to the respective business, holds for commercial corporations, companies and especially for operators of critical infrastructures and indirectly also for vendors. The citizens of the Information Society, as far as security in general and the dependability of infrastructure and services specifically are concerned, can simply assume the consumer role. This means the citizen can request security and dependability any time and any place, but is not obliged to contribute in any way to activities that assure this dependability or security.

The Basic Requirements of the Citizen

The European citizen’s requirements, therefore, are mainly focused around an individual, personal perception of security and dependability and all its related implications. Individual, personal, democratic, self-determined control is much more important to citizens than the traditional, historic, government-controlled central approach to security and dependability. In the European Information Society, security and dependability concepts must take into account not only central control requirements but also the individual need for security and dependability mechanisms that protect the citizens’ privacy and identity. A research framework should pay special attention to areas of security and dependability that do not follow 20th century central command and control approaches, but that instead could lead to an open and trustworthy European Information Society in which the end user is empowered to determine his or her own security and dependability requirements and preferences. This need for self-determination is accompanied by a need for a reliable, dependable infrastructure that such self-determination can be applied to. Processes of the Information Society will be digitized more and more and there needs to be a reliable, failsafe communications environment and infrastructure in place to support these processes. Within this environment, the roles that the citizens can take will be multiple ones: anyone can act as a private person, as an employee, as an economic agent on behalf of an organisation, a national citizen, a citizen of the European Union, a member of any social or political group, or just as an anonymous user of information services.

The citizen’s perspective on security and dependability can, therefore, centre on the requirements to protect all the assets of the virtual Information Society that contribute to an individual’s personality and existence in real life. These requirements can be illustrated by the following questions:

- The uniqueness of the identity - *Who am I?* and *Who are you?*
- The ability to decide – *What can I choose?* and *What can you choose on my behalf?*
- The privacy of personal knowledge and history – *What do I know?* and *What do you know about me?*
- The ability to act – *What can I do that is right?* and *What can you do wrong?*

- The ability to control – *What can I do to protect myself from risk?* and *How can I manage this risk*?

Consequently, a Security and Dependability Research Framework for Europe’s Information Society technologically needs to take into account the electronic equivalents of the above cornerstones of individual existence, namely Digital Identities, Channel Management, Information Privacy and Infrastructure Dependability.

Organizations' Perspectives on Security and Dependability

Notions of security and dependability have always to be interpreted contextually. For example, an event that is seen as a security lapse or a computer system failure within a particular corporate department may be dealt with so successfully that the corporation as a whole will not regard itself as having a security or dependability problem. Alternatively the problem may not be containable within the department, and higher levels of the corporation may have to become involved in coping with the situation. But if this can be achieved without any stakeholders external to the corporation being affected, the corporation's overall security and dependability will remain intact. Indeed, the very definition of what would constitute a security lapse, or a dependability failure, depends on context - one organization's incident can be another's disaster! In other words corporations today specify their needs for security and dependability as statements that express which risks are acceptable and which risks must be reduced. The capability of dealing with security lapses and dependability failures is hence planned as contingency actions for risks that might or might not have been mitigated.

As indicated earlier, organizations vary greatly regarding their security and dependability needs. However all – from governments, government departments, universities and research organisations, large corporations, NGOs, SMEs, etc., – have, in common with individual citizens, a need to maintain and manage their overall identities, and to try to retain effective ownership of their information assets, and to protect and benefit from their rights. All organizations that rely on others when executing their business processes have therefore a fundamental interest to understand the levels of security and dependability (i.e. "trustworthiness") that their partners exhibit, and thus the type and level of trust which it is reasonable to place on them.

Expressing these security and dependability levels in contracts for business process outsourcing, say, is one of the fundamental problems that are too often neglected. As a consequence, the corresponding service level agreements fail to reflect what is expected. Renegotiating the contract or even moving out of the partnership causes not only costs but also usually leaves the buyer with years of delay. Hence, security and dependability need to be quantified requirements in service level agreements that focus on both liability (the motivator) and design (actions to reduce/eliminate risk by design).

Organizations vary regarding the extent to which they can take effective responsibility for meeting their security and dependability needs, protecting their information assets, etc. And the degree to which they are able to exercise a level of effective control, for example by legal or financial means, over individuals within the organisation, or even outside it, may vary greatly. But it is always unwise for any organization to ignore or deny the realities about citizens outlined in section 2.2 above. Central to the needs of stakeholder individuals in the Information Society are the problems of Digital Identities, Channel Management, Information Privacy and Infrastructure Dependability. They are even more important to the stakeholder organizations, being responsible for their own interests and those of their clients – they apply directly to the organisation's identity management problems, and it is in the best interests of every organisation to see that the needs of individuals in that organisation, or interacting with that organization, are properly provided for.

In regards to being compliant to (IT) regulations European corporations are facing a particular problem. It is currently almost impossible to specify a common European baseline for IT compliance requirements, which means that European corporations (in terms of compliance costs) cannot scale with the market size.

In the above, security and dependability were discussed as though they are always evaluated from a balanced point of view. But it is important to recognize and address the challenges that arise when commercial players explicitly DO NOT WANT other stakeholders to have security, regarding it as being in their interest to prevent this for purposes of control and profit. (An example is when providers of payment cards integrate themselves in commercial transactions between commercial entities instead of incorporating security features such as Digital Cash or other means to reduce risk and enable trustworthy transactions. The service providers thus become the primary source of risk as is seen with identity fraud related to credit cards and data collectors.) In fact, one finds these kinds of potential conflicts when the issues of Empowerment and Dependability are disregarded or omitted for commercial purposes. For example, in DRM, infrastructure channels, and “trusted party” identity schemes, and “trusted computing” products whose goal is less about the protection of the actual user’s interests but more about safeguarding the assets of major suppliers of infotainment and functional software.

Such conflict of interest problems have research dimensions (we need to ensure the potential availability of trustworthy solutions), a market dimension (someone needs to bring trustworthy solutions to market) and a regulatory dimension (if the market does not solve security problems themselves, regulatory steps have to be considered). In fact, market and security by design approaches need to be to be the primary focus as moving to regulatory means in security can often lead to unbalanced approaches in which the main risks are left to regulatory protection alone, and situations in which enforcement proves in practice difficult or even impossible. Focussing on ensuring that liability is relocated to those able to deal with the problems is much more effective.

In summary, Empowerment and Dependability are closely interrelated issues, and focussing on Citizen Empowerment in fact helps to address the concerns of all stakeholders.

Core Concepts and Their Issues

Digital Identities

Related to the aspects of privacy is the citizen’s, and in principle every stakeholder's requirement to act in multiple different roles in the Information Society. In contrast to the natural individual identity of a person or an organization, the Information Society is composed of virtual, digital actors that are distinguished by a multitude of identity schemes. Already today, mechanisms such as social security number, bank account number, credit card number, cell phone number(s), business e-mail address, private e-mail address etc. are used by individuals as alternative identifier schemes for different purposes. Sometimes such an identity might quite appropriately lead to a set of persons using the same equipment and services, such that there is no longer a clear one-to-one and not even a one-to-many relationship between digital identities and natural individual identities. Similarly, organizations sometimes need only be identified via their current role, and may be identified differently in different environments. It is, therefore, vital to distinguish between the individual (or other stakeholder), the device, and the communication channel within the overall, integrated picture.

In recent technological research, there have been numerous approaches to the employment of biometrics for security purposes, building on the uniqueness of biometric bodily characteristics and the easy availability of biometric devices. Biometrics has played, and will increasingly play, an important role in crime forensics and in non-repudiation but also for self-protection and proving innocence. What is critically important is to recognise that the goal should not be identification and surveillance but the balance of security needs. For instance biometrics is problematic for use for authentication as the “secret key” is not secret, revocable or unique, – biometrics can be spoofed and victims of identity theft cannot get a new set of biometrics, and using several spoofable biometrics can merely create more “fake security”.

Empowerment considerations involve ensuring that the use of biometrics in Identity and key management is based on easily and securely revocable keys such as private biometrics (biometrics locked in mobile tamper-resistant reader-devices) or bio-cryptography (integration of biometric characteristics in revocable cryptography keys) while enabling the use of a plurality of identity schemes. Indeed, empowerment and dependability are not achievable if control is always with someone else and attackers commit identity theft based on faking biometric credentials – an old type of crime that will grow in a world where identity credentials are increasingly used.

Fake identities and identity theft are considered one of the most important issues for the citizen - but in fact are equally important to organizations, such as banks, given the current prevalence of so-called "phishing". In the information society of the future, the breakthrough regarding these issues for transactions and electronic processes will be two-fold: there will be some services that can be used anonymously in community-based or information-retrieval scenarios where there are only loose virtual trust relationships and there are no valuable goods involved. (For example in Blogs or Wikis, such environments can already be seen today.) The other core area of the Information Society contains those electronic processes that have an emphasis on valuable, goods or service transactions. This we typically find in commercial or government-related applications.

For the scenarios as described above, stakeholders may feel a need for validated traceable identities to execute a transaction, such as registering with the tax authority. However, to make such identities useful, they need to be interoperable as well as mutually recognized (e.g., federal government & municipal government). In addition, citizens' and often organizations' privacy must be protected, which may require anonymous and unobservable access, e.g. to a news system, an interactive communication system, or a telephone counselling service. Whilst proper accounting in the case of using pseudonyms must be assured as well. Naturally, this also necessitates a well-balanced handling of contradictory requirements for law enforcement and data protection.

Considering the above is vital insofar as citizens might be willing to provide certain information freely, if benefits are forthcoming (e.g., customer loyalty scheme). In such a scenario, pseudonyms or limited identities must be used that enable citizens to restrict secondary use and control which information they wish to provide it to the merchant, for what purpose and for how long. This is currently not the case for the problems outlined above. Thus, there will be a continuing potential of conflict between merchants and citizens. One potential conflict might be that a citizen feels that the seller only needs to know payment information without their personal details appended. However, the merchant might want things that are not truly necessary from the citizen's viewpoint. In fact, the latter may be willing to provide such information only if he or she can see a clear benefit from giving such information e.g., providing name and postal address to merchant to received ordered goods having no alternative way to achieving this. (Such concerns are perhaps most easily illustrated for citizen and/or consumer stakeholders, but analogous situations can occur, for example, among companies involved in sensitive business transactions.)

Channel Management

The concept of Digital Identity has to be seen as independent of but closely related to that of Communication Channels and Channel Devices.

Identities operate across communication channels and, therefore, need to be separate from such communication channels. At the same time, security and, in particular, accountability, in a channel is closely related to who is using the communication channel rather than the actual channel device being used.

Re-use of the same channel identifiers leads to uncontrollable linkability of identities or transactions, something that presents a serious problem in a digital world. For instance, citizens in their homes have no real protection when using persistent IP addresses. Basic services such as search engines link and profile increasing amounts of data for advertising and other commercial purposes often in databases whose users cross legal borders. If citizens, or any other stakeholders, enter into commercial or government transactions, re-use of communication channel identifiers leads to similar problems.

A key problem is that identifiers collected in one context can be used for attacks in entirely different contexts, so leading to problems such as Distributed Denial of Service attacks, *phishing* attacks or viral attempts to take control of communicating devices for various criminal purposes, with Identity Theft as the most serious problem.

A key and increasingly important focus for secure and dependable ICT must, therefore, be on how to ensure communication channels do not restrict stakeholders', and in particular citizens', security. It is necessary to align this with use of Digital Identities. At the same time, accountability and security against abuse have to be taken into consideration. Issues such as usability, identity credentials and interoperability between identity management and channel operators will continue to grow in importance until suitable solutions have been found and implemented.

Information Privacy

There is a major concern to assure privacy of the individual in particular, though various other categories of stakeholder typically also have privacy concerns. Laws and regulations in the European Union have supported the European approach to data protection, but the citizen might have individual privacy requirements that go beyond these. Data aggregation and data collection are clearly a problem already, and problems such as computer worms, spam mail and phishing have shown how misuse of data that are not necessarily person-related can be highly annoying to the citizen and even block electronic processes that had already established themselves as a habit in business and private life.

The privacy, security and dependability requirements of the citizen are, therefore, much broader than the pure protection of personal data and the continued accessibility of critical services. Any transaction that is performed in the Information Society, any process that is established electronically and any service that is offered over ICT must be trustworthy, i.e. dependable and inherently secure. This can also mean that the citizen can justifiably trust (in the sense of 'depend on') that certain information flows do *not* happen - or by design only happen in a way where citizen retains control. In a privatized, decentralized and dispersed communications environment, the number of central control organisations will significantly decrease. Nevertheless, citizens should be able to determine whom they are willing to trust (for what purposes, and to what extent), but there can also be a large set of parties involved in services and processes, such that a trust decision might be highly complicated or even impossible for citizens to make. Similar concerns also apply between other categories of stakeholder, such as a set of SMEs that have temporarily come together to form a virtual trading organization. The Security and Dependability Research Framework for the future Information Society, therefore, should pay special attention on approaches that provide mechanisms for trust in a heterogeneous, untrustworthy environment.

One should *not* assume that stakeholders do not care about their security merely because they do not understand the consequences of certain actions. The perception of risk can vary significantly from actual risk and, in the short term, convenience may lead some early adopters to make hazardous decisions. But just as we see serious problems with excessive distrust and concern preventing or impeding the take-up of key technologies, e.g. GMO and mobile phone masts, misplaced trust in a system can eventually lead to serious security and dependability failures if such naive trust is used as an excuse to ignore basic individual security.

Data or identity security in critical and value-creating ICT cannot be maintained through regulatory instruments alone, as enforcement is increasingly impossible, impracticable and ineffective. There is a need to move instead to a more integrated approach, incorporating self-protection and built-in security using context-dependent identity and channel management to separate and isolate each stakeholder's different transactions or roles.

The Applications and Services considerations

The service-centric view emerging from the development of service-oriented architectures (SOA) is changing the way IT infrastructure and applications are and will be managed and delivered. This will affect information society's stakeholders in ways that cannot be ignored, and poses challenges in several domains, not only the technological ones.

Applications will utilise components out of different domains of control and will be obeying different policies asking for diverse security and dependability qualities, since they will be offered by a multitude of providers. In fact, contrary to the current situation, components may be owned and operated by many different organisations, and services shared between many consumers. Monolithic perspectives of system security, already challenged in current networked and distributed systems scenarios, must give room to modular and decentralised perspectives representing the reality brought by SOA[18]. and more flexible identity schemes empowering the stakeholders to reduce risk to them.

In such scenarios, it is not surprising that confidentiality, integrity, availability, and QoS requirements will increase, or at least become more visible in service-level agreements (SLAs), which may be agreed in a dynamic and decentralised way, and may also provide for dynamic variation depending on instantaneous context. However, if nothing is done to tackle this situation, software and services will continue to be

[18] Whilst SOA brings new perspectives to TSD, it is recognised that SOA does not force any additional framework for more security in composing services and that such a framework has to be introduced explicitly, afterwards. This was a major conclusion at the ESFORS Workshop in September 2006 [8].

offered on a "best effort" basis, rendering the problem of fulfilling SLAs, and in general, of rendering correct and acceptable services, a very difficult one to solve. This amounts, to a great extent, to understanding how organisations can assure themselves, regulators, and customers, that they have appropriate control over their IT.

Risks of the move toward Services

Let us take the service level agreement (SLA) example, since it will be a crucial component of future service oriented architectures. An SLA is a contract. As such, there must be trust between the parties. Since we talk about services, we essentially mean the user trusting the service provider. Obviously, when a provider signs an SLA, it should have the means to fulfil it. The user, on the other hand, should believe the former has those means. But normally, the user is led to believe a more superficial predicate, that 'the provider will fulfil the SLA', regardless of the means. Moreover, details about these means are frequently considered proprietary, and, thus, not available to the user, even if it wanted to assess them.

Imagine the scenario of an application service provider (ASP), who signs an SLA with several clients. The ASP must guarantee certain conditions of quality of service as seen by Internet users, as well as non-functional properties such as security and/or dependability, both of users access, and of the information being stored and manipulated in the servers. The clients may be end clients, or in turn be online service providers, in which case they may themselves sign specific SLAs with their end users, which will reflect the conditions they get in the ASP contract.

Whilst it should directly guarantee that its data centre fulfils what is agreed, the ASP should contract an SLA with the Internet service provider(s), which in turn contract with their raw cable or wireless providers. On the other hand, some of the provisions the ASP contracts with the end user probably depend on properties of infrastructural services transparent to the former, like isolation effectiveness of virtualisation SW/HW, or protection/detection effectiveness of firewall/intrusion detection system compounds.

Such a scenario, which is quite simple, already implies a high degree of uncertainty both in what contributes to fulfilling the end SLA, and in whom to blame when things go wrong. The ASP is the visible tip of the iceberg, and, as things currently go, business practice ends up relying more on muscle (the aforementioned unilateral trust constructions) and legal advisors than on technical arguments and mechanisms, as it should. In a service-oriented architecture world, this can only get worse, and as such, requires methodical research on the methods, architectures and mechanisms to deal with the problem

Society and Policy Considerations

Continued adoption and trust in ICT-based services will depend largely on the user-friendliness of such services. However, 'ordinary' people find themselves having to deal with the well-known plagues of viruses, spam, rootkits and phishing attacks. Existing technologies, in order to protect from such attacks, will introduce costly barriers to the usability of ICT-based services, driving society away from their use. Security technologies that deal directly with people and society must remain user-friendly while being secure.

One complication often found is the combination of multiple trust sources at a country and European level. ICT-based services lack a framework of regulation that determines recommended or mandatory security requirements from a given service. This situation may degrade as we move to SOA, for the reasons already explained, but this may constitute an opportunity to address the problem in a thorough and generic way. The EU has already started to develop rules to secure electronic communications, principally, the *electronic signatures* directive, and *data protection* legislation for electronic communication. We need comprehensive governmental policies for software and services and systems that guarantee interoperation in a secure and dependable way.

Infrastructure Dependability

Empowerment of the stakeholder, and in particular the citizen, is of limited help when there is no environment around to apply it to. Today's Information Society already is heavily dependent on the availability and reliability of infrastructure (e.g. cell phones, wireless hotspots, E-Mail servers and xDSL lines, together with a vast variety of software systems whether running on desktop computers or shared servers). The future Information Society will be even more dependent, as the density of communications infrastructures will increase and new technologies are already on their way. Citizens and other stakeholders therefore need multiple and interoperable ways of access to communications infrastructures and environments provided by different parties. The topics of Critical Infrastructure Protection and Critical Information Infrastructure Protection will partly converge, as even very traditional physical infrastructures (e.g. roads or water supply) will be more and more controlled and managed by information networks. A large share of services will be offered electronically, and many processes that require personal interaction of the citizen today (e.g. renting a DVD, making reservations, identifying him/herself) will look completely different. Although the individual citizen, and stakeholders such as SMEs have limited control over the availability of communications environments and infrastructures, reliable infrastructure and service availability is nevertheless a key concern.

As already discussed, access to digital networks needs to be more related to the context of use rather than to the identification of people or devices in order to reduce the interdependencies and vulnerabilities that will lead to secondary problems due to any interactions.

From the perspective of the various stakeholders, and in particular that of individual citizens, the European Security and Dependability Research Framework, therefore, should address availability, reliability and robustness intensively. In doing so, a holistic approach should be taken that consider both traditional network oriented approaches and new technologies in order to create redundancy and improve service availability by increased interoperability between the different omnipresent, ubiquitous communications technologies of the future. Well-designed redundancy strategies are critical with respect to coping with physical faults and operational accidents, but the problems of possible residual faults, e.g. in complex software, especially faults that constitute exploitable vulnerabilities, require sophisticated fault prevention and removal strategies, as well. Fundamental to the success of such strategies will be the extent to which developers manage to identify and remove undue system complexity. To resolve and make security interoperable in heterogeneous devices and protocols, these essentials security elements should be characterises through a semantic characterisation and definition.

Technologies for security provision

A fundamental requirement is the development of basic security technologies, that include cryptology, multi-modal biometry, secure and dependable software and hardware development, trusted functionality, intrusion detection and prevention, etc. There is a broader need to develop integrated taxonomies, models and tools to capture requirements, support design, verification, integration and validation. It is beyond of the scope of this document to provide an extensive treatment of all these technologies and, therefore, we focus on those considered to be the most fundamental: cryptology, trusted functionality, biometry and the interactions between them.

In order to be effective, the implementation of the techniques provided by cryptology requires a trusted or trustworthy environment – variously referred to as trusted computing, trusted execution, trusted platform, etc. The intention here is not to debate who controls what, but point out the dependency. Quite obviously, conventional cryptography carried out in an untrustworthy environment or agent is of little value[19]. In addition to research in cryptology itself, two related areas, trusted computing and relationships with biometrics, are addressed below.

Cryptology developments

Cryptology, the science, and cryptography, the practical application of the science, are fundamental to provision of most aspects of security in communications and IT systems– and as a consequence also their dependability.

Work on modern cryptology has been in progress for many years now, delivering results on which much of our information infrastructures are dependent for their current, albeit imperfect, security and dependability. But now, in addition to responses to fundamental issues such as quantum computing, with its potential to invalidate many of our current approaches, the current, and forecast increased, rates of expansion of information flows require new and improved results from the cryptologists.

[19] this is not to deny the possibility of trusted cryptography by untrusted components – hence *conventional*, which may be simply by-passed or spoofed unless further checking were used – but this would then provide some degree of the required trust

Numbers of devices are spoken of in billions, and information in terabytes. The implications for cost, performance, simplicity, energy needs, etc. are, to say the least, demanding. In addition to the mathematical science aspects, the requirements for supporting implementation technologies and engineering will have their own challenges when it comes to delivering the goods.

Envisaged developments – ambient intelligence; fully dynamic, heterogeneous, converged communications, GRIDs, etc. – present new challenging applications, which need to be addressed by different or better crypto solutions and methods than the ones we have today.

Some further specific crypto challenges are listed in section **Error! Reference source not found.** below.

Trusted functionality

Trusted computing provides cryptographic functionalities in which a trustworthy system can be built, where trustworthiness is defined according to the underlying security policies. Today, one instantiation of these functionalities is provided by a core component called trusted platform module (TPM) and can be used to (i) remotely verify the integrity of a computing platform (attestation and secure booting), (ii) bind secret keys to a specific platform configuration (sealing), (iii) generate secure random numbers (in Hardware), and to (iv) securely store cryptographic keys.

In this context, there are various research issues to be explored:

Security model for the components used on a trusted computing platform such as a TPM: For future developments, it is important to establish an abstract model of these components and their interfaces to be able to analyse the security and cryptographic as well system-related mechanisms that rely on the functionalities of these components.

Efficient multiparty computation using tiny trusted components which have only a limited amount of storage and provide only a few cryptographic functionalities as mentioned above: Many interesting applications like auction and voting may require complex cryptographic protocols or still inefficient computations for their realization depending on the underlying trust model and the security requirements. It is interesting to examine how and to what extent trusted computing can improve the existing solutions.

Property-based attestation: the attestation functionality allows one to verify the configuration of an IT system. This, however, raises privacy problems since one may not be willing to disclose details about the internals of an IT system. In this context, property-based attestation would only require an IT system to prove that it has a configuration of a certain property, *i.e.,* it conforms to a certain (security) policy instead of revealing the configuration itself. Here, one can prove the correctness even if a configuration changes but still obeys the same policy. For this, we need to design efficient cryptographic mechanisms.

Maintenance and migration: using trusted platform modules also require methods and mechanism for transferring complete images (of applications and operating system) from one computing platform to another. Here, one needs to design efficient and secure mechanism to move a complete software image between platforms with different TPMs and different security policies.

Integration of Cryptology with Biometry

Due to its convenience and reliability, use of and research into biometrics is increasing rapidly in recent years. However, privacy and security problems, such as exposure of personal information, identity theft, abuse and counterfeiting of biometrical data and irrevocability, arise. Using cryptology can contribute to effectively protecting biometrical data from these risks. In addition, biometrics provides unique, and possibly irrevocable and incontestable identification of the human being. Integration of cryptology with biometrics can build direct connection between users and their passwords or keys in security system in order to avoid the unpleasant experience of having to remember and use different passwords, risks of sharing and stealing passwords or keys.

Combining cryptology and biometry improves security and convenience of system. However, traditional cryptology cannot apply to biometrics since biometrical data cannot be produced exactly. Research into development of new cryptology for noisy data would then be needed to address this. Techniques such as perceptual hashing and the derivation of keys from biometric data using additional helper data (referenced and/or metadata) are very promising. The combination of biometrics and cryptology with steganography and digital watermarking also offers new opportunities for secure and user-friendly identification protocols that offer better privacy.

There is direct relevance of this area of work to the progress of the management of digital identity discussed in section **Error! Reference source not found.**, above. Some further specific crypto challenges are listed in section **Error! Reference source not found.** below.

Research areas to be addressed

Introduction

The Advisory Board has taken a bird's-eye view of the results from the Security and Dependability Task Force (STF) and aggregated different challenges around *nine* key areas, extended from the seven areas originally identified by the STF [Annex II]. The results from the Security Task Force add more detail, and provide substantial technological aspects to the Research Framework. The SecurIST Advisory Board recommendations should be seen as high-level advice based on the set of key areas that the Security and Dependability Research Framework should address.

It is clear that information and communication systems, which are key to the functioning of the European Information Society, consist of both technical and non-technical components. The technical components include software and hardware contained in devices, PCs, servers and communications infrastructure. As important as these technical components are, they are not the whole story, and for an information system to function properly, a number of other non-technical factors have to be addressed. These include factors concerning people and their behaviour, such as policies, procedures, best practices, standards (regarding people), risk management approaches, education, training and socio-technical aspects. The Advisory Board believe that it is important for these non-technical factors to be addressed within the Security and Dependability Research Framework.

The nine key areas identified by the Advisory Board are as follows:

1. Empowerment of the various types of Stakeholder, and in particular of Citizens
2. Europe-specific Security and Dependability
3. Infrastructure Reliability and Availability
4. Interoperability
5. Processes for developing more secure and dependable systems
6. Security and Dependability Preservation
7. End user centric Standardization
8. Security and Dependability of Service Oriented Architecture
9. Technologies for security

Each of these areas is outlined below.

Empowerment of Stakeholders

Stakeholders' and especially citizens' perceptions of security and dependability are and will be heavily influenced by their awareness of the need for security and dependability and their trust or distrust in the services that *Information Society Technologies* deliver. Therefore, user and especially citizen-centric aspects of security and dependability should be a core element of any new security and dependability concept for future information and communications technologies. There is an obvious conflict in paradigms between the traditional central command and control approach to security and a new, user-centric approach. As all central server systems have to open up and integrate with other systems and technologies to enable the benefits of digital society, the classical assumption of large centrally controlled security systems fail with the concentration of risk and growing complexity. Either the access control models will become unmanageable or so high level that surveillance security will become unmanageable and still won't be able to prevent penetration of the increasingly less protective perimeter security. Security has to be semantically enriched and control distributed to protect the central systems security. This results in many questions regarding how to satisfy the differing needs of central organisations such as network operators, governments or law enforcement agencies and simultaneously leave room for self-determined, user centric control of security and dependability.

The Security and Dependability Research Framework should pay special attention to the citizen-centric approach, as under the general threat of terror, there seems to be a temptation to fall back into traditional, historic security concepts based solely on central command and control. Of course, there might well be legacy structures and environments that require central control and for which there is a continuing requirement. But even such environments need to start now to address the new technological challenges of the future Information Society, as they will clearly face competitive technological environments of tomorrow (such as e.g. peer-to-peer communications, self-organised networks or ad-hoc communications) that do not depend upon central control structures. Consequently, in an ever more complex world, citizens and other end users must be better enabled to control the flow of their personal information. As leaked information is almost impossible to "retrieve", sophisticated mechanisms are needed for anonymity, for user-controlled release and for transfer of information. Could the individual be granted rights and controls equivalent to those sought by commercial organizations through DRM?

Procedural knowledge – describes the user's applied knowledge and skills regarding how to proceed under particular circumstances regarding the protecting of informational assets. Such knowledge is accomplished after some substantial training and practice of the skill has occurred. The saying 'practice makes perfect' applies here whereby more training improves not only the speed but also, most importantly, correctness of the action invoked. As a result, if a certain context occurs as reflected in hands-on training, the appropriate response can occur quickly and without requiring substantial mental processes to do so.

Technical means for controllability – describes the user having access to the necessary tools and resources for being empowered to control the risk for data-veillance and data shadowing. One of the challenges is the increase in number of near-invisible devices as part of the "Internet of things" where Citizens have to be able to control devices without interfaces often operating almost autonomic.

Technical means and procedural knowledge has to be aligned - Education about both security risks and tools to remedy these risks go hand in hand with ensuring empowering tools. Tools without education of usage or understanding of purpose will not work. Understanding of and modelling tools according to human mental modelling of security is also critical as increasing complexity – ceteris paribus – means less ability to manage security risks unless the identity paradigm moves beyond simple identification assuming someone can be "trusted" just because they are identified.

Semantics across different technologies, protocols, devices and security/identity models are critical for users to have manageable security while enabling developers to fulfil their obligations of service level agreements. Applications need to define their security requirements in much more flexible terms as they can often not predict which kind of devices and protocols, they will interface towards. Semantic descriptions and dynamic security resolution with built-in user empowerment will be critical for achieving simultaneous improvement of security and increase flexibility and distribution.

Empowerment represents a careful balance between the user's wish for convenience and simultaneously the need to control who will get access to what information, and when (e.g., interests, online activities and mobile). Moreover, ambient networks provide increased risks for data shadowing while providing greater convenience for users.

The view of identity as such has to move beyond mere Identification towards more nuanced concepts of identity. Government create and enforce a system of basic Identification, but if this is not integrated with empowering user-centric identity management, then National Id turns into systemic security problems and loss of autonomy. The route ahead is not to avoid structured identity and National Id, but to find ways to move beyond SINGLE National Id in both the private and public sector into at least a two-layer model, where on top of trustable Identification is built interoperable and trustworthy identity providing dependable Empowerment of the Citizen with the purpose of protecting BOTH the central systems, the citizen and society interests.

While solutions to the above may be manifold, including but not limited to digital identities, the current trend towards centralising of management and control represents a challenge to empowerment of citizens beyond the digital age. The research needed under this heading will, perhaps more than any other issue discussed in this report, require the *people sciences* as well as technical expertise and insights. Adequate understanding of how existing systems are used, misused, ignored or abandoned requires the expertise from psychologists and sociologists, as well as from the relevant technical areas. Moreover, such understanding is a pre-requisite to the successful development and deployment of future systems that the European stakeholder will trust and use appropriately.

Europe-specific Security and Dependability

The European Security and Dependability Research Agenda should have a well-defined position on how to align European approaches in comparison to other regions. Only the ability to take into account specific European structures, facts and histories will turn a European Security and Dependability Research Framework from a technologically focused framework that could well have originated from any other region on the globe into a framework that brings real added-value into the European Information Society. The European background that needs to be taken into account includes, but is not limited to, differing technological levels of the 27 Member States, historic trust and distrust relationships, flexible internal and external borders, different languages and different cultures.

The SecurIST Advisory Board, therefore, strongly recommends the pursuit of research into the direction of European Security and Dependability platforms[20]. Such platforms could be based on legislation, processes, practices, software, hardware, knowledge, capabilities or any combination thereof. As certain aspects of security and dependability are out of bounds for European regulation by mandate of the EU treaty [9], of course, the legal basis for any European Security Platform must be carefully validated.

From the stakeholder's perspective, Pan-European Security and Dependability Platforms could provide an added value to being a citizen or other stakeholder of the European Union, in contrast to being the citizen or stakeholder of a Member State only. Any such platforms should in coverage be limited to EU stakeholders but should provide interfaces to approaches from Northern America or Asia: the notion of Security and Dependability Platforms could be seen as an equivalent to existing successful European competitive advantages such as the European Monetary Union [10], the European Economic Union [10] or the European border control system according to the Schengen treaty [11].

An example of a European security and dependability platform (or component) could be, e.g., a legal agreement and technical system recognizing citizen identity cards from all European Member States to serve as a platform for electronic access to government services across Europe. European Security and dependability platforms, of course, are not limited to technological systems but should also comprise skills networks, legal agreements or common awareness campaigns on security and dependability.

The major value of research on European Security and Dependability platforms is threefold: primarily, Europe-specific requirements can be considered more easily than in US or Asian approaches. This will create better solutions from a European perspective and ease the transfer of research results into the European market. Secondly, there will be measurable added value to the European citizen and stakeholder, who will be able to benefit from being a European citizen (by Europe-wide processes, services or agreements). Thirdly, the position of Europe in global competition will be strengthened if European Security and Dependability platforms can be embedded into global technology standards, processes and regulative frameworks.

Establishing European security and dependability platforms will, therefore, provide benefits to European citizens and stakeholders

- on a personal level (for being able to use broader platforms),
- on a European level (due to the pan-European coverage of these platforms), and
- on a global level (due to the global recognition of unified European security and dependability platforms).

Infrastructure Robustness and Availability

The Information Society is becoming increasingly dependent on ICT infrastructures such as mobile and ubiquitous communications, location based services and the Internet. From the perspective of the stakeholders, the reliability and availability of ICT services will become increasingly important, although the individual, as an end-user, may not wish to pay too much attention to technical background infrastructure.

[20] the term *platform* refers here to one or more commonly usable sets of hardware, software, processes, policies, practices, knowledge, capabilities or any combination thereof, and is not supposed to be used in the traditional meaning of "technical system" only.

Converging ICT technologies have started to enable broadband mobile internet access at any time and any place, and many existing legacy processes have been be transferred to electronic platforms and networks. The requirement to address reliability and availability, and indeed overall dependability issues with high priority will, therefore, not be limited to new and converging network technologies and standards. Moreover, it will also be imperative that software and system vendors deliver products, which are perceived as parts of the infrastructure by the citizen, to meet specific dependability responsibilities. Careful adherence to best practice, and to avoiding undue system complexity, will be critical.

Beyond the citizens' direct perspective on ICT, there is an additional demand for reliability and availability facilities and services in the control plane of critical infrastructures that affect the every day life of the citizen. Classical critical infrastructure sectors such as medical, energy, telecommunications, transport, finance, administration and first responders [12] will become an integral part of the Information Society and the borders between the virtual and physical world will disappear. Dependability of critical infrastructure services will depend heavily upon reliable and robust control networks and mechanisms – whether this be for a traffic management system for congested roads or a load distribution mechanism for broadband mobile internet access. Mechanisms to preserve critical infrastructure control that need to be considered must not limit their scope to protection against accidental faults of designers and of operators or cyber crime attacks but cover all scenarios of infrastructure failure, including physical damage by major incidents, catastrophes or terrorist attacks.

Interoperability

In a secure Information Society, there will not be a homogeneous, standardized technology for communications purposes. Different fixed, mobile and converging technologies will address different requirements from very near field communications via body area networks to broadband broadcast communications across national borders. Security and dependability features and properties of communications systems need to be tailored to the specific needs of the respective communications environment and will ideally be built into the relevant specifications from the beginning. This means that there will be a large set of security and dependability mechanisms, serving similar goals in different environments. The communications landscape will be scattered and dispersed with a very large number of handover points and gateways between technologies. In such an environment, it is of the utmost importance to the end user not to have to cope with a large and complicated set of security and dependability features, but instead to have easy access to the platforms of the Information Society, including an interoperable and integrated security model. The Security and Dependability Research Agenda should respect the current trend towards decentralized and converging communication technologies by addressing especially the area of interoperability and integration of security and dependability mechanisms, technologies and standards. In particular, attention will need to be paid to improved techniques for identifying and removing "security gaps" in highly complex heterogeneous systems. Rather than focusing on "open" standards in meaning of Open Source or Open Processes, focus should be on the semantics of security by establishing and standardising on a meta-level able to cover much wider than merely one security model. The key problem is how to create interoperability between multiple security models for different purposes and enable new kinds of security and identity models for instance incorporating user empowerment. A focus on transparency through verifiable semantic will prove a vital aspect of both knowing and being able to resolve actual security assertions against application security requirements.

Processes for developing more secure and dependable systems

Ideally, security and dependability should be considered together and treated seamlessly from the first stages of any system design. However, the current reality is different: the development process for information and communications systems today is focused mainly on functional features, whereas security analysis and secure and dependable development are trailing in professionalism and investment in many areas. To avoid increased efforts in adding security and dependability to insecure systems, security and dependability should, where possible, be built into all information and communications systems from the beginning. (This applies whether one is constructing an entirely new system, or one composed out of pre-existing systems.)

This requires a broad approach mainly in the area of software development: threat analysis, risk analysis and the use of appropriate security and dependability architectures should become mandatory in the development process, and software developers are to be educated regarding proper security and dependability design and security and dependability pitfalls. Furthermore, automated software development tools must be provided that include fully or partly automated handling of security and dependability issues as well. Security and dependability in the sense of proper software development covers not only such traditional aspects as authentication and encryption but will rather also aim at proper handling of various specific issues such as e.g. buffer overflow mechanisms, tailoring systems to the end users needs and omitting superfluous functions that might become security and dependability risks. Handling of access rights according to the need-to-know principle and an easy-to-understand management of security and dependability parameters will also be required.

Research on the effectiveness of security and dependability awareness programs with regard to system architects and developers should be done in parallel to see how efficient the measures can be.

The end user perspective is that systems developed according to certain secure and dependable development standards or best practices could achieve a higher level of trust for their stable and reliable security and dependability.

Security and Dependability Preservation

In contrast to the considerations about availability of services for the citizen described in section **Error! Reference source not found.**, the increasing complexity of Information and Communications Technologies imposes another challenge for a European Security and Dependability Research Programme: in a more and more complex environment, the stakeholder, and specifically the citizen must preserve his/her security and dependability without needing to become an expert in security and dependability. The increasing number of technological standards and the large number of new technologies, all intertwined, partly overlapping, partly complementing each other and in special cases already converging, make it a special challenge to maintain security and dependability at an adequate level across all components as new systems are introduced. The Information Society will not only use standards that are well-defined, tested and approved by the community but will always be driven by early adopters of new technologies and products. Security and dependability – with a perspective of being as strong as the weakest link in the chain of an interconnected Information Society – is in great danger of falling behind the technological development in the high-speed, short time-to-market scenario sought by the industry.

Preserving security and dependability also means preserving predictability in an uncertain environment with respect to multiple facets of technology: uncertain synchronism, fault model, and even topology. On the other hand, systems are required to fulfil more and more demanding goals, which imply predictability or determinism, e.g. timeliness, resilience, security. Systems, therefore, must be capable of adapting, and they must do so in a more or less predictable and agile/dynamic manner. Moreover, they must retain the good qualities they provided, and above all, any confidence users had in them, mainly with regard to sensitive aspects of information privacy, transaction correctness, etc. The balance of the required predictability and the uncertainty of the environment is a major challenge to be addressed. On the other hand, forward thinking must not be hindered by a lack of security or dependability. The European Information Society of tomorrow will be stronger and more capable with every solid technology platform successfully deployed in the market. GSM in the 1990s has shown that such quantum leaps are possible, and emerging standards, technologies and products with a European origin (e.g. Galileo) might have the opportunity to repeat this success story. Ultimately, a European Security and Dependability Research Agenda should take into account the necessity to maintain security and dependability in an ever more complex and de-centralized technological environment. Current approaches such as high level security and dependability description languages, end-to-end security and dependability, and security and dependability standards already point to one possible direction to address this challenge. Additional approaches are urgently required to provide a stable security and dependability basis for new technologies and to offer seamless, plug-and-play, high level security and dependability to the citizen.

User centric Standardization

Standardization is one of the cornerstones of a pervasive and secure Information Society of the future. For seamless ubiquitous ICT to become reality, technological interoperability and gateway functions are required. This will only be possible on a basic foundation of standardized or de-facto standardized services and technologies.

Today, standardization is mainly concerned about technological issues and is driven by experts from technology vendors and operators. As the operator role will change in the future due to a trend to more decentralized technologies, the citizen end-user will partly become involved in issues that used to be operators' business before. Therefore, end users should be represented as stakeholders in standardization activities.

Unfortunately, as of today, only very few consumer or end-user representatives have participated in standardization activities (only slowly and on specific occasions, e.g. in the ENISA advisory board or in the SecurIST Advisory Board, first end-user involvement becomes visible). To tailor a more decentralized security and dependability model in the future Information Society to the needs of the citizen, end-user associations and representatives should be more involved in standardization activities. This will require, in all probability, both programmes of awareness raising, and financial assistance aimed at levelling the standardisation playing field.

Security and Dependability of Service-Oriented Architecture

Further to the research challenges already identified in the previous sections, SOA will further stimulate the need to develop logics and mechanisms for building trust on a given service based on the perceived notion of the actual trustworthiness of several, and sometimes disparate, underlying infrastructure modules. Given the fragmentation that SOA imposes on the classical notion of “system”, these relations may well have to develop recursively. Furthermore, given the characteristics of SOA, the above-mentioned relations must include assurance, socio-technical, policy and regulatory aspects.

As ICT systems become more complex and interdependent, it will get ever more difficult to manage security and dependability unless appropriate action is taken. The use of service-oriented architectures (SOA) is intended to increase the business agility that today's organizations need in building federated services; However, at the same time, it is required to provide the visibility and control necessary for underlying horizontal issues such as security and dependability. Additionally, current standards for best practice and security management (e.g., ISO17799/27001) must be adapted to the generalised scenario of outsourcing deals, sub-contractors, etc. expected in an SOA world. Legal, risk and auditing aspects may be important in this endeavour, to study how to share risk/security and dependability information between providers.

We need appropriate models to: configure, change, and assess the security and dependability of aggregated services and information sharing; drive the definition of SLAs; and make assurance cases about their fulfilment. In essence, it is important that we devise mechanisms to establish and maintain trust and manages policy regulations and service contracts such as SLAs, in an SOA context.

Despite the advent of service oriented architectures and the challenges identified above, the quest for seamless integrated security and dependability must continue. Traditional security and dependability protocols alone do not provide seamless and integrated security and dependability across multiple protection domains. New paradigms based on SOA must emerge. The complexity of context-aware privacy and security protection from both the user and the application layer is bound to increase, and needs to be hidden behind appropriate interfaces. Techniques such as virtualisation of personas, devices and services may well be required, as users move across multiple trust and services domains.

Trusting Service Level Agreements in an SOA context

Even with the fairly stable, centralised and visible notion of provider that characterises current business practice, it is already difficult to provide formal technical guarantees about the *capacity* of the infrastructure and supported services to meet given SLAs. Likewise, for services deployed over the Internet, user trust is more of a question of faith, largely based on political/social factors, such as reputation (standing in market), insurance (endorsing responsibility to third parties) or inevitability (monopoly, public administration) of the provider. The provider in effect says "Trust us, you know us!" or "Trust us, you have no other option!"

One might argue that this situation, awkward as it may be, is unsatisfactory to the users but rewarding to the providers. In fact, this is not true. Providers are the visible face to the end-users, but normally they are, equally, users with respect to other providers, and thus the problem has repercussions throughout the value chain. And unfortunately, the situation will become unsatisfactory, if not unsustainable, to all stakeholders, in an SOA context, if nothing is done to improve the situation. In a service-oriented architecture world, there may be many different participants dealing directly with one another, components may be owned and operated by different and possibly many organisations. In fact, a real application service provider setting may end up being implemented by a multitude of access, Internet, and hosting providers, lying behind as many federated component service providers.

Services will be shared between many consumers; components will obey different and independent security and dependability policies, increasing the risks considerably. If we wish to maintain the traditional approach, we will end up buried under an unmanageable number of SLAs. The most basic reliability theory tells us that failures will be more frequent if we pursue the current "best effort" approach, that SLAs will fail, that the capacity and responsibility (or lack thereof) of service providers will be brought under the spot lights, and that (irresolvable) conflicts will be the rule rather than the exception. In such a deregulated and finely granulated world of components, the fragile *trust* building described earlier risks falling apart.

This brings us back to the crucial problem: users are *forced to place* trust on the services they buy, whereas they should be given *evidence* that allows the *building of* that trust That evidence is very much concerned with the *trustworthiness*, i.e. the *security and dependability,* of the services and obviously, of the infrastructure supporting them. Service providers must provide evidence that they can fulfil the SLAs they sign. This capacity should be auditable by regulators and other authorities. The user should be given means to build trust, either by directly assessing the capacity of the provider, and/or by a transitive relationship with regulating bodies that are trusted by the user, and which can assess the provider's capabilities and capacities.

In an SOA context, all these are research challenges, and the problem has several facets:

- how can users and other stakeholders obtain fixed guarantees about the capacity of providers, as current assurance standards are insufficient for SOA?
- how can organisations assure themselves and regulators that they have appropriate control over their IT to keep it dynamically within agreed parameters?
- how can systems enforce and assess at run-time the individual trustworthiness of components, and be able to include them in trustworthy systems, in particular systems that provide the desired degree of security and dependability against faults, attacks and intrusions?

The future needs to achieve a much closer correspondence between *trust* on the applications as seen by users, and *trustworthiness* of the infrastructure and supporting components. In this future Empowerment will be a key means to enable trustworthiness in ICT, and thereby the means to enable user trust. In essence, this all boils down to the study of the technical (system mechanisms) and legal (standards and regulations) means of guaranteeing, "a service running on S is trusted only to the extent of S's trustworthiness". This is believed to be a key factor of success of business in an SOA world.

Service engineering

There are ongoing requirements for advances in our ability to design and implement trustworthy services, applications, and software infrastructure – fundamental developments in software engineering calling for R&D for:

- construction and composition of secure services;
- secure service engineering and service deployment;
- assessment – verification, validation, etc. – of correctness, security, and dependability of provided services.

Technologies for security

Behind the foregoing requirements for further R&D in specific key areas is the need for development of the intrinsic technologies – the foundations and building blocks that will support everything else. We can build nice secure models of this and that on our laptops, but when it comes to the real world we need the proper bricks and mortar, steel frameworks, and reinforced concrete. Higher levels of assurance will be sought for the components of the dynamic, heterogeneous networks that will deliver ambient intelligence.

An important challenge in the development of basic technologies is the creation of a common language (taxonomy) and of models and tools to capture requirements, support design, verification, integration and validation of security solutions – the red and green pencils[21] are objects from a distant past.

Two fundamental security technologies that need to be addressed are

Cryptology – to protect information stored or transmitted outside of a 'home' trusted[22] environment, and even to provide certain trustworthy interfaces within that trusted home;

Trusted functionality – a generalisation of trusted/trustworthy (footnote **Error! Bookmark not defined.** still applies) hardware, trusted platform module, micro-code, intimate/kernel software, and basic aspects of operating systems up to some specified API; this can be used to construct a trusted local environment – trusted to do certain specified actions, and only those actions; it can ensure that information is handled by it and within it only as intended; as discussed earlier, the implementation of the cryptographic processes themselves needs this sort of trusted execution environment.

A third area is that of the protocols that utilise the cryptography, as well as manage it. These are interactions between entities to achieve certain security goals. In addition to key-agreement protocols that allow for authentication of entities and for the establishment of key material, cryptographic protocols can achieve much more complex goals: in principle parties can compute any function of information they share while protecting the privacy of their inputs and without the need to trust a single central entity; this is even possible if certain parts of the players are compromised, hence protocols that use these advanced techniques are potentially much more robust than simple protocols in use today.

Work in these areas has been in progress for many years now, delivering a stream of essential results, but the need for billions of ubiquitous, cheaper, smaller, faster, lower power, dependable components implied by the AI vision will place further demands not only on the technology and engineering, but on the underlying physical and mathematical sciences.

Crypto challenges

Specific challenges for cryptology research include:

Crypto-everywhere: software, hardware, and nano-scale implementations will be required as cryptography is deployed as a standard component of all communication and computation layers and – with ambient intelligence (or pervasive computing) – at "every" physical location. Requirements will be for lower cost, higher performance, specific applications, smaller size, low complexity, provable correctness, and low energy consumption.

Long-term security: Many crypto-systems considered robust have been broken after a certain amount of time (between 10-20 years). For instance, most of the hash functions developed before 1993 have been broken. We need to build crypto-system that offer long term security, for example for protecting financial and medical information (medical information such as our DNA may be sensitive information with impact on our children, our grandchildren and beyond). In the medium term, we need to be prepared for the eventuality that large quantum computers could be built: this would require an upgrade of most symmetric cryptographic algorithms and a completely new generation of public-key algorithms.

Provable security: cryptography has been very successful in developing security models and security proofs within these models based on a limited set of assumptions but more work is needed to expand

[21] the complete technology support for the first multi-layer silicon and printed circuits

[22] *trusted* in its rather simple-minded interpretation as in TCSEC, etc., rather than the semantic edifices currently under construction, but based on some demonstrable claim to trustworthiness

this approach to more areas in cryptology; automated tools to assist in developing and checking such proofs seem a promising research direction.

Secure implementation: even if we are able to get theoretically sound cryptographic algorithms and protocols, most of their failures can be found at the implementation level. A design methodology and technical solutions to increase resistance to side channel attacks (power, radiation, timing attacks) and work on secure APIs would be very relevant.

Digital rights management: several techniques such as fingerprinting and watermarking are available and there is a growing interest in this area. However, there is a lack of solid scientific basis (even just openness about techniques used in commercial products) and insufficient academic research.

Privacy: diffusion of sensing, location based services, explosive growth of storage capacity and communication mechanisms, and data mining technologies present a major risk to privacy. The problem lies in the asymmetry of technology: advances in technology make privacy violations much easier, while protecting privacy is complex and delicate (integrated solutions are necessary that work at all layers – physical, network, transport, application). Ease of use plays an important role here too. Advanced cryptographic protocols can bring substantial advances in this area.

Long term security and dependability

Security and dependability issues typically go along with the life cycle of a technology. The trend to first deploy a technology and later fix its problems – typically driven by economic motives – is gradually making way for security by design, resulting in improved security at the beginning of the life cycle. Unfortunately, the security issues of a technology near the end of its lifetime are typically overlooked. The best known example is that of cryptographic keys and algorithms (cf. supra) which may need to offer in some cases security for 50 to 100 years. However, this problem also arises in other areas such as electronic documents. Will it be possible to view current documents 50 years from now and, if so, will it be possible to assert their integrity? Many applications stay in use for much longer than anticipated, but during the extended lifetime they will be functioning in an environment for which they have not been designed, resulting in completely new vulnerabilities and risks. For example, software may be running on a processor that can change its instruction set on the fly or new tools may become available that allow to circumvent or evade security boundaries. In view of the complexity of the challenging security and dependability problems we are facing today, addressing these issues seems to be far beyond the state of the art.

Preview – a longer term vision of research in security and dependability

Overview

In addition to the need for short- to mid-term R&D in the nine key areas identified above, it is also essential that a forward watch be maintained that looks out for the possible developments arising from new or emerging technologies as well as new applications of existing technologies. In other terms, we have to build on top of these nine key areas and provide much longer-term reflections and views on how the research community may address crucial issues related to the evolution of the Information Society in the coming 10 to 20 years ahead. Four future *grand challenges* are given below as examples of where possible (r)evolutionary developments might be anticipated. The purpose of this section is to provide a vision for longer-term cross-disciplinary research in security and dependability.

Digital security and dependability is a discipline that is continuously evolving, with widening deployment of digital (fixed, mobile, wired and wireless) technologies, and their penetration into all aspects of human activity.

The goal of the fast expanding area of Security and Dependability research is to strengthen the secure circulation of data on robust networks, the computations of information on secure and dependable computers within a resilient ambience, promote the dissemination of computer applications and encourage the adoption of digital technologies by the general public, and provide effective means of trust and risk management.

Computing is not a discipline that is governed by the laws of nature[23]. It is a pure creation of the mind, with all its advantages (inventiveness, originality) and faults (errors of strategy, price-fixing, forecasting, specification, design, validation, operational use, etc.).

To grasp the complexity and follow the construction of these digital structures, new abstractions must be created in order to devise new efficient paradigms. It is also necessary to design new models, production tools with new languages, and protocols with modelling, simulation and verification techniques.

In order to construct resilient architectures of large evolutionary systems made up of independent heterogeneous elements that are context aware and fault-tolerant, have adaptive behaviour and take into account mobility, dependability and security, we need the following:

First, research on **new computing, communication and information models**, taking into account security and dependability, and their enemy, system complexity.

Second, the **injection of semantics** into these systems, because in a mobile, changing world, information must be validated **locally**. These models must be sometimes discrete, sometimes continuous and sometimes stochastic to envisage the future and explore the environment.

Third, the creation of **interaction models and knowledge models** so that independent devices can, during their life cycle, learn how best to interact; also **models for creation, acquisition, distribution, sharing of knowledge and trust**.

With all these diverse models, it will be possible to design and build new architectures, new protocols, and new trusted infrastructures.

To carry out such work, we need also to spend efforts on **languages and tools**. This involves the creation of programming and markup languages and tools, interaction languages and tools, in order to inject security and dependability during the design phase. New dependability, security and trust infrastructures with separated instrumentations and processing are required, in order to better grasp the digital activity, and to better understand the validity and the quality of trust. It is also necessary to develop protocols in much more flexible and decentralized networks that will break the monotony and symmetry of network nodes, with algorithms of cooperation, coordination and autonomy, thus resolving issues of scale.

[23] apart from the fundamental law of engineering: *what can go wrong probably will*

Finally, **assessability** (**verification and validation) techniques** need to be developed.

Security and Dependability – four Grand Challenges

In this section, four future *grand challenges* that security and dependability science must take up in future years are described as examples of where possible (r)evolution might be anticipated. These challenges are based on a cross-disciplinary perspective and reflect the preparation of appropriate reaction to potential future dark visions and golden opportunities; they are not entirely imaginary, but contain very real possibilities. Underlying R&D directions on which they are based may appear to be FET-like research and beyond, but the outcomes will be very tangible. The security and dependability community needs, therefore, to be vigilant on these possibilities, analysing options for response to consequent opportunities and threats.

Countering vulnerabilities and threats within digital urbanization

The **first grand challenge** is the security and dependability improvement for the expansion and globalization of digital convergence by 2010-2015. In our way to this, we will notably observe three inter-related phenomena: *first*, the boundaries between physical space and cyberspace will start fading away; second, the dependence of citizens and organizations on ICT will increase so that it is crucial to enhance Critical (Information) Infrastructure Protection; and *third*, threats and vulnerabilities will increase while service availability will likely decrease. More specifically, when we consider the figure 99.9…9% of availability for a system or a service, the question is how many 9s are required and how many will be really implemented?

The above can be translated to the following open problems for the security and dependability community to resolve.

- ***how to move from "claustro-security" (closed and ciphered world) to an "agora-security" (open and clear world)?***
- ***how to move from static and standalone activities to a collaborative, network centric architecture vision with full mobility and full interactivity with people and reality?***
- ***how to make the actors' chain proportionally responsible and accountable for malevolent or erroneous actions?***

The evolution is towards ICT infrastructures that are globally interconnected and becoming the economic nervous systems of the modern world. The information society is, thus, becoming ever more complex but also more fragile. On the one hand, cyber terrorism and computer piracy will also set to increase. They will threaten our society and affect the daily lives of our citizens, the management and lives of our enterprises, and the operation of states. On the other hand, a vast number of interdependencies are progressively being built between the different information and communication systems and the various areas of human activity, such as administration, banking, energy, transportation, public health, or defence. New means for reducing the vulnerabilities due to the technical interdependencies are critical calling for security by design, citizen empowering and other ways to ensure damage control to both internal and external stakeholders.

Two trends seem then to emerge:

- Dependence on vulnerable, interdependent, interconnected, complex ICT systems: the information society evolves towards a more interconnected and standardized world. This evolution is characterized by an increasing use of 'open' communication infrastructures, such as the Internet, but also by a widespread use of monoculture software applications. This brings about vulnerability to all kinds of accidental or deliberate incidents and aggression, and their rapid propagation through heterogeneous infrastructures that operate more and more interdependently and under the same standards.
- Real-time resilience and security: The future evolution will involve technical, behavioural, organizational and even psychological changes, as evidenced by the growing dependence of our everyday activities on ICT systems. Companies are said to be agile, with short reaction loop decision cycles and just-in-time procurement cycles. Meanwhile, security also evolves towards just-in-time (software and antivirus developments). However, its effectiveness will be more and

more precarious and there is a need to move towards real time reaction capability to face the growing threats. The security of the dynamic reconfigurability and update of hardware and software at runtime is a major challenge for the years to come.

Overall, the security, dependability, privacy, interoperability, compatibility, administration, and life cycle of these heterogeneous and interdependent infrastructures are open questions.

Duality between digital privacy and collective security: digital dignity and sovereignty

The **second grand challenge** concerns privacy issues of all the players – citizens, groups, enterprises, and states.

There are always two angles of view in terms of security: the point of view of the user who wants to protect himself against the network or some entities there (this is the digital privacy standpoint, with a requirement for the preservation of individual freedom) and the point of view of the network or society, that needs to protect itself against malevolent and irresponsible users (this is the ambient security standpoint, with a requirement for the protection of the community).

The question for the ICT usage is the assurance of digital sovereignty and dignity for citizens and groups.

- ***how to override the "big Brother" syndrome and the dark security?***

One can thus picture the subtle and tough competition between, on the one hand, the methods designed to preserve a subject's privacy, , ensure empowerment and the legal procedures to watch such subject and, on the other hand, the practices intended to preserve the rest of the world against the potential malevolent or accidental acts of such a subject, and the latter's remedies to find out what means are being implemented to control him and to counter those means. Creating a climate of mutual respect and trust is not detrimental to the setting up of mutual defence cross-procedures. Transparent dialectics should make it possible to negotiate the rules and subscribe to clear and harmonious security policies. Such digital dignity is the price to pay for the democratic values of our civilization but citizen empowerment and means for better balances between accountability in a context and preventing the linkage of outside context represents one example of a way to reduce or eliminate the assumed problem.

Objective and automated Processes

The **third grand challenge** is the obligation to attain a controllable and manageable world of complex digital artefacts by 2015 toward a provable security (predictability of faults, anticipation of threats).

The challenge is the measurability issue:

- ***how to inject regular, quantitative techniques and engineering to make the field truly scientific?***

Beyond the Horizon: a new convergence

The **fourth grand challenge** is the preparation of a new convergence at a horizon of 2020 and beyond, which is the bio-nano-info-quantum "galaxy".

In this perspective, we may observe the decline of the present IP/3G/Google Age by 2010-2015 and perceive a disruptive appearance of new infrastructures by 2015. Currently envisaged IP may not be sufficient to support the next generation of wireless infrastructures (2015). The 3G/post-3G will likely be replaced by more open and interoperable infrastructures (2010-2015), and the content galaxy (information, multimedia, programs) will likely be replaced by new services (2015). During the next twenty years, we will partake in a long digital twilight and a novel re-emergence of "analogue" systems with combinations of atomic engines (nanotechnology) and/or living cells (bio-geno-technologies).

The emergence of bio-nano-infospheres will create a (4D+1D) multidimensional intelligence and disruptive mechanisms for the 21st century. A full new interface for security and dependability between those four universes (living + physical + digital + quantum) will have to be invented.

The big question will then be:

- ***how to protect the interfaces and to attain and maintain a security continuum?***

References

[1] European Commission's Regulation 2005/516 of April 22, 2005.

[2] http://www.enisa.eu.int/Engberg, S., Workshop presentation at Security Task Force Workshop 19th April 2005. http://www.securitytaskforce.org/dmdocs/workshop2/stephan_engberg.pdf
Additional: Trust In the Net Workshop (09 Feb. 2006) report available at
http://www.egov2006.gv.at/Reports/Report_Trust_in_the_Net_Vienna_09_FEB_06.pdf

[4] SecurIST Deliverable, D3.2 Validation Workshops report (Non - public version), November 2005.

[5] Veríssimo, P. E., and Neves, N. F., and Correia, M. P.: Intrusion-Tolerant Architectures: Concepts and Design. In: Architecting Dependable Systems. Springer-Verlag LNCS 2677 (2003). Extended in Technical Report DI/FCUL TR03-5, Department of Informatics, University of Lisboa (2003). http://www.navigators.di.fc.ul.pt/it/index.htmwww.itu.int/internetofthings

[7] SecurIST Deliverable, D3.1 ICT Security & Dependability Research beyond 2010 Initial strategy (Non - public version), October 2005

[8] ESFORS September 2006 Workshop report
http://www.esfors.org/downloads/ESFORS_Workshop_200609_Report_v1.3.pdf

[9] http://europa.eu.int/eur-lex/en/treaties/dat/treaties_en.pdf; Additional: http://europa.eu.int/eur-lex/en/treaties/selected/livre106.html (Article 23)

[10] http://www.absoluteastronomy.com/reference/economic_and_monetary_union

[11] http://en.wikipedia.org/wiki/Schengen_Agreement.

[12] EU: CI^{2}RCO Project www.ci2rco.org; European CIIP Newsletter -
http://www.ci2rco.org/ecn/European%20CIIP%20Newsletter%20No%201.pdf;
Additional references: US Department of Homeland Security report
http://www.whitehouse.gov/homeland/book/sect3-3.pdf, page 30
Canada: http://ww3.psepc-sppcc.gc.ca/critical/nciap/nci_sector1_e.asp
UK (MI5) http://www.mi5.gov.uk/output/Page76.html
Germany (German only): http://www.bsi.de/fachthem/kritis/KRITIS_Einfuehrung.pdf).
and many others.