IST Advisory Group
Trust, dependability, security and privacy for IST in FP6

Report

June 2002

Information Society Technologies

European Commission

IST programme

Report of the IST Advisory Group concerning

Trust, dependability, security and privacy for IST in FP6

http://www.cordis.lu/ist/istag.htm

A great deal of additional information on the European Union is available on the Internet.
It can be accessed through the Europa server (http://europa.eu.int).

Cataloguing data can be found at the end of this publication.

Luxembourg: Office for Official Publications of the European Communities, 2002

ISBN 92-894-3836-3

Printed in Luxembourg

PRINTED ON WHITE CHLORINE-FREE PAPER

CONTENTS

1. INTRODUCTION

This report, which is timed to coincide with preparation for the launch of the Sixth Framework Programme, has been prepared by the Information Society Technologies Advisory Group (ISTAG) that provides independent advice to the Commission on orientations and priorities for Community funded research activities.

In a parallel report on "*Strategic Orientations & Priorities for IST in FP6*" ISTAG anticipates that during the next ten years a new infrastructural paradigm will emerge — the 'Ambient Intelligent Space'. This is the collection of infrastructural technologies, applications and services that will enable the seamless interoperation of the applications and services of Ambient Intelligence.

ISTAG has considered the implications for security in this new paradigm. While the new paradigm offers a significant opportunity for Europe, there are also some deep research questions, and implications for the management of that research.

In this report ISTAG makes four recommendations for the direction and management of security-related research in the Sixth Framework Programme. These recommendations are fully in-line with the Resolution of the Council of the European Union of January 2002, in which the Council "*stresses the need for more research activities, in particular on security mechanisms and their interoperability, network reliability and protection, advanced cryptography, privacy enhancement technologies and security in wireless communications*" (2002/C 43/02).

Throughout this report, the word 'security' will be used as shorthand to encompass trustworthiness, dependability, privacy, rights protection, usage restriction, availability, confidence, integrity and secrecy.

2. BACKGROUND — THE NEW SECURITY PARADIGM OF *AMI SPACE*

In the ISTAG concept of Ambient Intelligence, intelligence is pervasive and unobtrusive in the environment. This environment is sensitive to the presence of living people in it, and supports their activities. People, physical entities, and their agents and services share this new space, which encompasses both the physical and virtual worlds — the Ambient Intelligent Space — or *AmI Space*.

In this space, people will participate in a multiplicity of parallel, overlapping, inter-leaved and evolving one-to-one, one-to-many, and many-to-many relationships, some of which will be very short-lived, and some of them established temporarily and (apparently) instantaneously. Much of the communication between participants in these relationships will be asynchronous (as it is now): this means that 'virtuality' applies to time as well as space.

Security in this space will require solutions very different from those of today's systems which are predicated on relatively stable, well-defined, consistent configurations, contexts, and participants to the security arrangements.

This new paradigm will be characterised by 'conformable' security, in which the degree and nature of security associated with any particular type of action will change over time and with changing circumstances and with changing available information so as to suit the context. This is fundamentally different from what has gone before and there are significant opportunities to enhance the competitiveness of European industry by exploiting this change in paradigm. ISTAG recommends that these opportunities should be seized if Europe wishes to maintain an independent capability in the field of security.

Meanwhile, within the existing security paradigm there are significant outstanding problems that inhibit development of information society markets. The majority of potential users of services and products have, at best, a poor understanding of security, which leads to caution and, at worst, severe distrust. They need comprehensible mechanisms in which they can have confidence. They must be able to depend upon reliable and available services, themselves dependent on reliable and available infrastructural equipment and applications, in an era of ever increasingly complex systems and constantly changing technology.

At the same time, content providers, who could provide the greatest stimulus for adoption of technology, are reluctant to do so given their present poor protection from abuse of the Intellectual Property associated with their content.

There is a difficult balancing act — to encourage research and development so that Europe is well-positioned to exploit the new paradigm; to continue to resolve problems within the present paradigm; and to research and develop applications and services which will probably eventually have to operate within the new paradigm, while having, for now, to work with the concepts, techniques and tools of the present paradigm.

3. RECOMMENDATIONS

Recommendation 1. If Europe wishes to have an independent position in security, or even to acquire a lead position, the route should be via the new paradigm of security, which will be required intrinsically in the 'Ambient Intelligent Space'.

The key features of this new paradigm are described in the *'Background'* of Section 2, above. A more detailed exposition is given in Annex 1 — *'Security in the AmI Space'*. Some of the research required to realise this new paradigm is described in Annex 2 — *'Research issues for security in AmI Space'*.

Recommendation 2. We must not lose sight of the present reality, and the pressing problems in the present security paradigm which must still be addressed.

Within the present paradigm of firewalls and certificates, security issues have not yet been 'solved' and Information Society markets are therefore not as well-developed as might be hoped. The Framework Programme must continue to research solutions to these problems, some of which are discussed in Annex 3: *'Unresolved security issues within the present paradigm'*.

Recommendation 3. We need to migrate to the new paradigm, without eroding existing market positions: actions within FP6 should recognise this and be designed so as to accommodate such migration.

ISTAG suggests that one of the roles of the proposed specific advisory group (see next recommendation) should be to monitor the mix of old and new approaches to security, and to foster the development of advice and guidance to projects on how migration might best be achieved.

Recommendation 4. A specific advisory group should be established so as to facilitate a dialogue between the parties affected by security concerns in order to advise the Commission on the direction of security-related actions in FP6, and on appropriate related actions outside FP6.

This group should be supported by research projects to address particular security problems, and co-ordination actions to gain synergy from communication and cross-fertilisation among researchers, and to inform the wider community on possible mechanisms to enable security in the *AmI Space*.

The group should liaise with other activities of the Commission and Member States to facilitate Community and international co-operation, as sought by the Council of the European Union (2002/C 43/02).

4. OPTIONS FOR SECURITY-RELATED ACTIONS IN FP6

Solutions to the problems posed will require a very different set of approaches to security from those deployed at present, and will require changing the mind-set of much of the community. With this in mind, ISTAG has considered a range of options for management of security issues in FP6.

If there are several separate integrated projects, with security requirements in each, then there is likely to be much common overlap. If they are not to be integrated or co-ordinated in any way then they could possibly have incompatible outcomes. But is it feasible to co-ordinate projects that are already individually very large?

Moreover, projects will be starting soon; there are problems waiting to be addressed within the existing paradigm; and the new paradigm requires research before the ideas can begin to be put into practice. **So projects must begin within the current paradigm and yet be aware of the likely need to fit into the new paradigm as it emerges.**

The following options were considered:

1. Offer advice and guidance on security issues to all appropriate projects in FP6.
2. Establish a special initiative on security, using either or both of the FP6 instruments of the 'Integrated Project' or 'Network of Excellence'.
3. Require that each integrated project has a trust rationale and a specific security package, and specify a range of issues which that package must address, including the need to ensure harmonisation of proposals and developments coming from the collection of projects.
4. Establish a high-level advisory group of experts, reporting to the Commission, to guide FP6 projects on security issues, to commission targeted study and research, to provide a service to projects, and to raise industry awareness on the trust/confidence/security issues.

Note that these options are idealised: in reality there could be other intermediate possibilities and mixtures of all these.

ISTAG has concluded that:

- Mere guidance is unlikely to have sufficient impact.
- A major stand-alone security-oriented initiative would run a serious risk of being too detached from the other projects, and perhaps from the market, resulting in a further set of incompatible outcomes rather than a common — or at least harmonised and interoperable — solution.
- A requirement for 'security packages' for each project — which are intended to lead to coherence across the whole programme — is thought to be unmanageable.

- Given the complexity of the issues and the need to achieve coherence while allowing diversity of research, a high-level advisory group is essential. Among its roles it might stimulate other activities.
- **Some mechanism is required for rapid communication within the community of latest understanding of requirements and emerging solutions, for both the present and the future, *AmI Space*, paradigm. To achieve this a co-ordination action should be established to act as the 'operational arm' of the high-level advisory group.**

Composition and operation of the specific advisory group

Such a group could be a sub-group of the future EAG (Expert Advisory Group) for the IST priority under FP6, augmented by non-members of the IST EAG when appropriate.

It is important that an advisory group on security does not become closed-minded and a constraint on new thinking. To avoid this membership should be broadly-based with representation not only from experts in the field but from 'users' — those who wish to provide or use products or services that depend on security. Above all, its membership should represent the position that ***security should be an enabler for the development of new markets, not an inhibitor***.

The composition and operation of the group should reflect the ambition of the Commission, as expressed in a recent Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, which reads:

> *"The Commission is proposing to include security in the future 6th Framework Programme, … For this spending to be optimal, it should be linked to a* ***broader strategy for improved network and information security.*** *Research supported by this program should address the key security challenges posed by the "all digital" world and by the need to secure the rights of individuals and communities."* (COM(2001) 298 final)

The membership should also take into account the need to operate at the ERA level, in support of the ambition of the Commission and the Council of the European Union to enhance Community and international co-operation in the quest for improved information and network security.

The proposed group should not merely offer advice: it should be *effective* in shaping the programme and its content. To this end there must be a rich flow of information to and from the group, and members of the group should either participate in the processes associated with the programme (such as evaluation) or have liaison with those who do.

In particular, the group should both inform and be informed by project reviewers (especially those for the major Integrated Projects). Not only would this help to achieve a coherence of vision across FP6, it would also help to keep the group sensitive to the latest thinking in the field.

Annex 1: SECURITY IN *AMI SPACE*

In order to be able to solve security issues in the coming decades it will be necessary to move from previously held points-of-view on security. In the 21st Century, we must escape from the influence of the Internet, GSM and the like, and their security paradigm based on von Neumann and Shannon models, however successful they may have been and however much they provide the basis for the new *AmI Space*.

Security — A growing concern

As we build the AmI Environment, security will become more and more a concern because of:

- Size: in pervasive computing there are millions of subjects and objects
- Mobility: which introduces more vulnerability than in a static world
- Heterogeneity: no longer can closed, co-designed systems be assumed
- Complexity — of both hardware and software, increasing the dependability challenge
- Distribution of knowledge coupled with co-operation as more and more groups will be interconnected and work together.

In addition, in the coming years, quantum communications may emerge, to communicate securely using chaotic models. This may well change the way that security is implemented through large networks, even in the present paradigm.

Security is also acquiring new *dimensions*:

- Ethics — the concept of illicit content is already extant, but soon we will have to consider the ethics of computations. Today computations are still considered to be private, but this attitude is unlikely to persist
- Reliability — of critical infrastructures (perhaps with survivability areas …)
- Resilience — in a hostile environment we must avoid the delusion of security behind a robust barrier, and continue to operate despite threats and despite actual, successful, attacks.

Even more fundamentally, security in the AmI Space will require a new *nature*.

The new nature of security in *AmI Space*

In *AmI Space*, ambient networks with objects and subjects will be moving all the time, without physical connections in many instances, and without standard identification, since anonymity — which is orthogonal to security — is often required. Mobility in *AmI Space* implies not only *nomadic people*, but also mobile *things* in the environment, such as constantly-moving

intangible agents which manifest themselves to users through such things as caches, liquid software, and downloadable applications.

With current security models, we consider security only in the context of salient subjects, Alice and Bob, talking together in an isotropic world, independently of the context, and of time and space. But consider the following scenario:

> Alice (a friend of Bob) is moving at some speed on some trajectory to her office and is talking with Bob who is elsewhere, travelling elsewhere in his car.
>
> The communication takes time — a few minutes — and the confidentiality between Alice and Bob changes during the conversation (e.g. trust is low at the beginning, high at the end for Bob, because Alice is convincing; but it is the contrary for Alice who terminates the conversation with some doubts …). Part of the conversation is intimate; the other part just needs integrity (updating their agenda for the day) with no secrecy; and all the conversation is done in a noisy environment with poor availability of the communication channel.
>
> It will be similar for software agents — 'Astrid' in a client-server mode with 'Batiste'. Security enforcement will depend on the stages of co-operation between the two applications.

Subjects can be physical individuals or the related programs that they run, but can also be computers, printers, or routers that do a certain job in the cyberspace. Objects can be files, documents, or content (voice, image, video, database, etc.). Subjects can perform operations on objects. These operations will be licit or not, depending upon the region of the ambient intelligence space. These subjects and objects are autonomous, though not independent. Subjects move through this cyberspace and meet other subjects with other security policies. When they meet together, they negotiate their joint security policy.

The old OSI model based around client-services and fixed bilateral relationships between people is disappearing. In today's mobile world, relationships are both open and closed**. In AmI Space, security policies cannot be defined top-down. Security must be defined for each 'salient' subject and object in each region of the cyberspace by a security policy which takes into account the locality — in space and time.**

Security policies in this environment must evolve, adapting in accordance with our experiences. Such approaches may be very different from present approaches to computational security policies, but may better embody our approaches to real-world person-to-person trust policies. This is the main new feature of the new paradigm for security in *AmI Space*.

Approaches to security in *AmI Space*

Solutions to these new security requirements are likely to lie in designing new intermediation services to manage the interfaces between telecommunications operators, users and service-providers, offering security protocols yet to be invented. They will need to support four new underlying ideas:

1. A medium exists, which is a cyberspace with ubiquity of communications (internet, GSM, 802.11, Bluetooth, etc.) and ubiquity of computations (grid concept, new distributed computing, disappearing computing, etc.). This is a mathematical space (along time t and space x,y,z) which is not isotropic but heterogeneous (in terms of communication, computation, etc). This space has, for each region, particular properties in terms of confidence, in terms of context …

2. We will no longer think in terms of 'bits of information' (Shannon digital bits with no semantics) but 'small programs' which are intelligent (with a Turing semantic) and which can decide their actions depending upon context. For example, a printer is no more just a piece of hardware to deliver a service, but a Java program with printing methods (Jini SUN concept); an IP packet is not a part of protocol data with a header and a user part, an IP packet may be considered as a Java program which may run on some router, during the trip through networks.

3. There are no longer only two sides to a communication (Alice and Bob, one emitter and one receiver), but instead there is an open set of individuals (Agate, Bertrand, Charlotte, David, Elodea …) who are co-operating in this cyberspace, exchanging information and sharing knowledge together. Members of this set are not necessarily all equal.

4. There is no central administration for this *AmI space*. This means that there is no single virtual machine to run all the applications, nor one single trust (and trusted) infrastructure. Instead there will be a distributed interactive infrastructure with a plural set of compatible local infrastructures.

Moreover, to implement security in this new world, we will need to relax constraints implicit in the preset paradigm:

- We must not presume a system which is either secure or 'breached', but one which allows resilient, survivable operation in the face of threats and actual breaches.

- We need not insist upon security enforcement at the time of a transaction or operation: we might instead take measures before or after. (For instance, with traceability one could perform a retrospective audit, and take appropriate remedial action.)

- We need not suppose that there is no confidence at all between two subjects, as is the case with current approaches to security — SSL,

cryptography, etc. — and therefore implement a full security protocol for ever. Most of the time this is not necessary. The level of security must be adapted to suit the circumstances — services on demand, protection of content … For some actions, we can envisage *ad hoc* and short-lived security — which can be broken perhaps after a few days for a standard conversation in normal life or after 3 months for a videogame CD-ROM.

The need for migration

Having said that we need to devise very different security solutions for *AmI Space*, we must recognise that the market requires safe and economic migration from today's techniques — encryption, SSL, VPN, Firewalls, smart cards, etc. — to the new, whatever it will be.

Annex 2: RESEARCH ISSUES FOR SECURITY IN *AMI SPACE*

ISTAG did not address *all* security problems, but instead focused on the problems which are not addressed within the present paradigm:

- How can we ensure that privately owned information can be shared to the extent which the owner wishes and no more; how can we detect breaches of confidence beyond this extent; how can we recover from security breaches; and what kind of remedies for such breaches can we provide? How should we deal with problems of transitivity and reflectivity (relations of trust when a request or an item of information travels across a chain of independent points of presence/nodes/links)?
- How can we manage the security associated with the multiple personalities and roles we will adopt in a multiplicity of relationships?
- How can we manage fluid, spontaneous co-operation, without imposed or predefined fixed roles and rules?
- How can we give the impression of seamless behaviour when moving through multiple and possibly heterogeneous environments?
- Can a trusted access capability be build into security protected environments, enabling emergency help (medical, fire brigade, police) to intervene efficiently in such environments (e.g. including, for example, the 'Personal Environment' when life-critical help is at stake)?
- How can we decide on the appropriate policies, strategies, architectures and allocation of resources in the absence of an assumed rationale for threats? (September 11th revealed that a presumption of a rationale for threats based upon economics is no longer valid: threats might have social or cultural motivations.) How should changes in rationale over time be seamlessly handled when they affect multiple environments?
- How should liability be linked to (breaches of) confidence in the chain from concept to operation of a device (perhaps embedded), system, network, or environment? The absence, from the inception, of confined liabilities may much later slow down or even divert deployment. Can we include liability in the design rationale?
- What *measures* are there, and what standards should there be, for dependability, trustworthiness, privacy ... ? We must accept that there can be no absolute guarantees of these attributes, and that measures might be probabilistic. Cf. SLAs. Should concepts like Design-to-Trust (DTT) or Design-to-Security (DTS) be developed in these matters, similar to Design-to-Cost in industrial design. And how can affordability be balanced with acceptability?

- How should we manage the relationship between identification and anonymity, so that authentification can be achieved without compromising privacy? Such management must allow optimal negotiation of relinquishment of privacy for efficiency of service provision, taking into account the needs of both the service provider and the consumer.
- How can unintentional breaches of security be tolerated and, how can help be provided to the user so that he can avoid the problem, while fighting deliberate intrusions?
- We need a better understanding of users of all kinds, including content and service providers, their customers, and the general public. For instance, do people use existing solutions? If not, why not?
- With Ambient Intelligence and communicating objects, with fluid local security policies, how can we be sure, or at least reasonably confident, that we will avoid pathological emergent behaviour of the total system, arising from interactions between people, agents, objects, and their various policies.

ISTAG makes the following observations:

- Any rules must be simple, user-understandable, user-friendly and intuitively usable.
- There must be societal acceptability, based on co-operation.
- Technology is not enough: any security-related initiative must address the issues of psychological perception by users, and the forthcoming security roadmaps should address issues of psychology and markets as well as technologies.
- Security should be:
  - an enabler of products and services, not a barrier to their introduction (cf. the way that safety has become a business enabler for cars)
  - a protector of national assets, not a barrier to their use.
- IST in FP6 should not over-focus on one facet of security, and should address:
  - security related to individuals: confidentiality, privacy, and data protection for personal information and programs, stored and running on networks, with control which is managed by the owner. Plurality aspects must be tackled, so that a person may authorize different people to have different restricted views on these data. This individual has several contexts (at home, at the office, in his car)

- security related to an open large community (with insiders and outgoers): how to share knowledge, along time, as the community evolve, as data and trust change
- security related to pervasive computing: security for very small communicating devices: new OS kernel, new protocols are required, with minimum security, but with the facility to enable more sophisticated security in combination with other devices
- security related to metacomputing (grid): security of large massively parallel computations
- security related to mobility and configurability: new models, new protocols are necessary for nomadic communities or mobile services
- security related to protection of commercial assets, including content, and control of access to them (This would be business-enabling). The concerns of the content provider, who wants his rights protected and a level playing field for competition, must be addressed as well as the concerns of the user. How can content be securely distributed online via Internet and mobile networks? What are the new models of communication (security of the transport) and of preservation (security of the use and access of the data at the user premises, etc.)?
- security related to large infrastructure: how to secure Internet in Europe, telecom operator infrastructures through Europe, national assets, large administrations, etc., taking into account their interconnectedness.

Annex 3: UNRESOLVED SECURITY ISSUES WITHIN THE PRESENT PARADIGM

Despite the exciting prospects for *AmI Space* and a new security paradigm, we must continue to operate within the existing paradigm for some years and attempt, through the Framework Programme, to resolve a wide range of issues which remain within the existing paradigm.

The need for online services with valuable content and the need for protection of content and security of services

WAP and GPRS have been less successful than hoped, with only limited markets, and UMTS may yet be a failure if there is no market for it.

Moreover, no-one should get carried away with the prospects for a new generation of intelligent services as the motivation for market growth: there is a 'chicken and egg' problem:

- most services are dependent on availability of content but content providers are reluctant to make content available on line because there is no market, and if there were, their content cannot be protected
- the market cannot develop because there is no content, and the potential user has no confidence in the privacy or security of the systems.

Availability of content might outweigh other fears (we all use Account Teller Machines while knowing of their security weaknesses), but this still requires that the content is provided, which in turn requires its protection.

We should consider both service *and* content, taking account of the interests of different players and business models. We need, through R&D, to find ways to secure online services (security of communication) and also to protect content once it has been distributed within the end user's device, whether TV set top box, PC, or UMTS terminal (probably using a preservation security model with access restriction, using internal hardware device, cryptographic protocol, or heuristics).

Psychological perceptions of security

It used to be the case that hackers attacked large organisations. Now, however, hackers are intruding on the individual's PC. As a consequence there is still very little confidence in the security of the Internet. Many users are, at present, uncomfortable giving a credit card number to a 'virtual shop'.

If the user experiences a security problem then they feel 'lost' — not understanding what is going on ('What *is* a digital certificate'?). Trying to

access one of our national web sites to make a tax declaration is reported to be a 'horrible' experience and even sophisticated users simply don't understand what is going on when they see security messages on their PC screen.

In France, Minitel is more trusted, because it is more comprehensible (or thought to be, by the users).

So, how might we render security more user-friendly?

The pace of change?

One hypothesis is that technology is progressing more quickly than people's minds can accommodate the developments. In the late seventies and early eighties only VIPs had phones in their cars. But the rest of the world wanted them and adopted mobile technology as quickly as it became available. But the latest changes are coming too fast for the market *and* they have no content.

However, there is a counter argument, that these things are not so simply predictable. In the late eighties the manufacturers doubted that there was a market for handheld GSM — that they would only be installed in cars and that the market would be only about 500,000 users. (Instead of the present figure of around 400 million.)

Is there indeed user-resistance to high rates of change? Could it be overcome? How?

How to avoid the problem of breaching barriers?

One reason for lack of confidence might be the prevailing 'firewall' approach which is secure as long as no-one has got through, but after that it is definitely no longer secure. In the new paradigm of an *AmI Space* the firewall approach to security is unlikely to be viable, but in the nearer term can we find other ways of managing security without such discrete vulnerabilities?

Interdependencies of infrastructures

The criticality of infrastructures has received much attention since September 11th. However, the interdependency between infrastructures — e.g. between power and communications — exacerbates the problem considerably. How should this be managed?

A 'point of trust'?

One counter to the problem of perception, adopted in Germany, is that one can give credit card details over the telephone and one need not pay

if there is a problem. On the Internet, though, it is not always clear who is responsible. Indeed, it differs from country to country. It is difficult to blame the operator — or even your ISP — if you get a virus on your PC.

A simple approach to all such security issues would be to extend the German approach and make the organisation to which one pays money be responsible for all aspects of security. Typically (at present, at least) this would be the operator. In that scheme, for instance, with regard to telephone gambling, it is the operator and not the gambling company which takes responsibility for security of transactions.

However, it is not clear that such a single focus will be evident in future in a complex of interoperating services. But maybe this needs to change so that *somebody* does take serious responsibility. This may not be the operator, and it may be difficult to define who *should* take such responsibility, but perhaps the concept of a 'point of trust' is important.

Can such a '*point of trust*' be established? If not in all situations, then in some? Are there prospects for a third-party '*point of trust*'?

Is the truly pervasive open system a delusion?

Frequently, security is enabled through proprietary systems (such as media-guard). It will be difficult to match such security on all-open platforms. On the other hand there is some concern that having private networks is, like the firewall, vulnerable to a single penetration. The ambition of many is to be able to have secure applications running over an insecure network. Is this *really* feasible?

Deregulation and fragmentation of owners and operators of secure systems

The multiplicity of operators since deregulation makes agreement and standardisation more difficult, so slowing market development. How might the processes be accelerated in this environment?

Dependability prediction and analysis of the whole telecommunication network

Currently, there are no scientific methods to model and predict the dependability of the whole telecommunication network, including terminals, for the new packet-switched protocols.

Anonymous incident reporting as a business accelerator

The nature of the security business at present is that it is difficult to know the true state of security of many systems because their owners and operators are unwilling to release information about security breaches. Moreover the

improvement of security is hindered similarly and by unwillingness to share information about breaches.

Would a palliative be to introduce a system of incident reporting, similar in concept to Air Traffic Control incident reporting, in which people who indicate security breaches would be protected? Intermediaries might be established to handle such reporting and its analysis sensitively.

Annex 4: CONTRIBUTION TO THE REPORT

This report was prepared by members drawn of the Information Societies Technologies Advisory Group, supplemented by experts selected for their knowledge of particular domains:

ISTAG members:

Angelo AIRAGHI — Chairman	Finmeccanica
Fred BOEKHORST	Philips
Kiril BOYANOV	Bulgarian Academia of Science
Alain BRAVO	Abhexis
Ezio BUSSOLETTI	Naval Institute of Napoli
Jose Luis ENCARNAÇÃO	University of Darmstadt
Håkan ERIKSSON	Ericsson
Michel FENEYROL	French Telecommunications Regulatory Authority (ART)
Philippe GEYRES	ST Microelectronics
Christos HALKIAS	Intrasoft
Michael HEALY	Ashling Microsystems
Tony HEY	EPSRC
Juhani KUUSI	Nokia
Paul LAGASSE	University of Gent
Carlos LOPEZ BARRIO	Telefonica
Soenke MEHRGARDT	Infineon
Paul MEHRING	ITEA Office
Gregers MOGENSEN	Consultant
Jean-Louis PIETTE	Groupe Lagardère
Ian PURVES	University of Newcastle
Stephen RANDALL	Symbian
Luc SOETE	University of Maastricht
Berit SVENDSEN	Telenor
Isabel TRANCOSO	INESC
Javier UCEDA	University Polytechnics of Madrid
Anita VAN LOOVEREN	OM partners
Hannes WERTHNER	University of Trento
Andrzej Piotr WIERZBICKI	Institute Lacznosci

Supporting experts:

Guenther HORN	Siemens
Michel RIGUIDEL	ENST

Rapporteur:

Bob MALCOLM

European Commission

IST Advisory Group — Trust, dependability, security and privacy for IST in FP6

Luxembourg: Office for Official Publications of the European Communities

2002 — 23 pp. — 21 x 29.7 cm

ISBN 92-894-3836-3

Venta • Salg • Verkauf • Πωλήσεις • Sales • Vente • Vendita • Verkoop • Venda • Myynti • Försäljning
http://eur-op.eu.int/general/en/s-ad.htm

BELGIQUE/BELGIË

Jean De Lannoy

Avenue du Roi 202/Koningslaan 202
B-1190 Bruxelles/Brussel
Tél. (32-2) 538 43 08
Fax (32-2) 538 08 41
E-mail: jean.de.lannoy@infoboard.be
URL: http://www.jean-de-lannoy.be

**La librairie européenne/
De Europese Boekhandel**

Rue de la Loi 244/Wetstraat 244
B-1040 Bruxelles/Brussel
Tél. (32-2) 295 26 39
Fax (32-2) 735 08 60
E-mail: mail@libeurop.be
URL: http://www.libeurop.be

Moniteur belge/Belgisch Staatsblad

Rue de Louvain 40-42/Leuvenseweg 40-42
B-1000 Bruxelles/Brussel
Tél. (32-2) 552 22 11
Fax (32-2) 511 01 84
E-mail: eusales@just.fgov.be

DANMARK

J. H. Schultz Information A/S

Herstedvang 12
DK-2620 Albertslund
Tlf. (45) 43 63 23 00
Fax (45) 43 63 19 69
E-mail: schultz@schultz.dk
URL: http://www.schultz.dk

DEUTSCHLAND

Bundesanzeiger Verlag GmbH

Vertriebsabteilung
Amsterdamer Straße 192
D-50735 Köln
Tel. (49-221) 97 66 80
Fax (49-221) 97 66 82 78
E-Mail: vertrieb@bundesanzeiger.de
URL: http://www.bundesanzeiger.de

ΕΛΛΑΔΑ/GREECE

G. C. Eleftheroudakis SA

International Bookstore
Panepistimiou 17
GR-10564 Athina
Tel. (30-1) 331 41 80/1/2/3/4/5
Fax (30-1) 325 84 99
E-mail: elebooks@netor.gr
URL: elebooks@hellasnet.gr

ESPAÑA

Boletín Oficial del Estado

Trafalgar, 27
E-28071 Madrid
Tel. (34) 915 38 21 11 (libros)
913 84 17 15 (suscripción)
Fax (34) 915 38 21 21 (libros),
913 84 17 14 (suscripción)
E-mail: clientes@com.boe.es
URL: http://www.boe.es

Mundi Prensa Libros, SA

Castelló, 37
E-28001 Madrid
Tel. (34) 914 36 37 00
Fax (34) 915 75 39 98
E-mail: libreria@mundiprensa.es
URL: http://www.mundiprensa.com

FRANCE

Journal officiel

Service des publications des CE
26, rue Desaix
F-75727 Paris Cedex 15
Tél. (33) 140 58 77 31
Fax (33) 140 58 77 00
E-mail: europublications@journal-officiel.gouv.fr
URL: http://www.journal-officiel.gouv.fr

IRELAND

Alan Hanna's Bookshop

270 Lower Rathmines Road
Dublin 6
Tel. (353-1) 496 73 98
Fax (353-1) 496 02 28
E-mail: hannas@iol.ie

ITALIA

Licosa SpA

Via Duca di Calabria, 1/1
Casella postale 552
I-50125 Firenze
Tel. (39) 055 64 83 1
Fax (39) 055 64 12 57
E-mail: licosa@licosa.com
URL: http://www.licosa.com

LUXEMBOURG

Messageries du livre SARL

5, rue Raiffeisen
L-2411 Luxembourg
Tél. (352) 40 10 20
Fax (352) 49 06 61
E-mail: mail@mdl.lu
URL: http://www.mdl.lu

NEDERLAND

SDU Servicecentrum Uitgevers

Christoffel Plantijnstraat 2
Postbus 20014
2500 EA Den Haag
Tel. (31-70) 378 98 80
Fax (31-70) 378 97 83
E-mail: sdu@sdu.nl
URL: http://www.sdu.nl

PORTUGAL

Distribuidora de Livros Bertrand Ld.ª

Grupo Bertrand, SA
Rua das Terras dos Vales, 4-A
Apartado 60037
P-2700 Amadora
Tel. (351) 214 95 87 87
Fax (351) 214 96 02 55
E-mail: dlb@ip.pt

Imprensa Nacional-Casa da Moeda, SA

Sector de Publicações Oficiais
Rua da Escola Politécnica, 135
P-1250-100 Lisboa Codex
Tel. (351) 213 94 57 00
Fax (351) 213 94 57 50
E-mail: spoce@incm.pt
URL: http://www.incm.pt

SUOMI/FINLAND

**Akateeminen Kirjakauppa/
Akademiska Bokhandeln**

Keskuskatu 1/Centralgatan 1
PL/PB 128
FIN-00101 Helsinki/Helsingfors
P./tfn (358-9) 121 44 18
F./fax (358-9) 121 44 35
Sähköposti: sps@akateeminen.com
URL: http://www.akateeminen.com

SVERIGE

BTJ AB

Traktorvägen 11-13
S-221 82 Lund
Tlf. (46-46) 18 00 00
Fax (46-46) 30 79 47
E-post: btjeu-pub@btj.se
URL: http://www.btj.se

UNITED KINGDOM

The Stationery Office Ltd

Customer Services
PO Box 29
Norwich NR3 1GN
Tel. (44) 870 60 05-522
Fax (44) 870 60 05-533
E-mail: book.orders@theso.co.uk
URL: http://www.itsofficial.net

ÍSLAND

Bokabud Larusar Blöndal

Skólavördustig, 2
IS-101 Reykjavik
Tel. (354) 552 55 40
Fax (354) 552 55 60
E-mail: bokabud@simnet.is

SCHWEIZ/SUISSE/SVIZZERA

Euro Info Center Schweiz

c/o OSEC Business Network Switzerland
Stampfenbachstraße 85
PF 492
CH-8035 Zürich
Tel. (41-1) 365 53 15
Fax (41-1) 365 54 11
E-mail: eics@osec.ch
URL: http://www.osec.ch/eics

BĂLGARIJA

Europress Euromedia Ltd

59, blvd Vitosha
BG-1000 Sofia
Tel. (359-2) 980 37 66
Fax (359-2) 980 42 30
E-mail: Milena@mbox.cit.bg
URL: http://www.europress.bg

CYPRUS

Cyprus Chamber of Commerce and Industry

PO Box 21455
CY-1509 Nicosia
Tel. (357-2) 88 97 52
Fax (357-2) 66 10 44
E-mail: demetrap@ccci.org.cy

EESTI

Eesti Kaubandus-Tööstuskoda

(Estonian Chamber of Commerce and Industry)
Toom-Kooli 17
EE-10130 Tallinn
Tel. (372) 646 02 44
Fax (372) 646 02 45
E-mail: einfo@koda.ee
URL: http://www.koda.ee

HRVATSKA

Mediatrade Ltd

Pavla Hatza 1
HR-10000 Zagreb
Tel. (385-1) 481 94 11
Fax (385-1) 481 94 11

MAGYARORSZÁG

Euro Info Service

Szt. István krt.12
III emelet 1/A
PO Box 1039
H-1137 Budapest
Tel. (36-1) 329 21 70
Fax (36-1) 349 20 53
E-mail: euroinfo@euroinfo.hu
URL: http://www.euroinfo.hu

MALTA

Miller Distributors Ltd

Malta International Airport
PO Box 25
Luqa LQA 05
Tel. (356) 66 44 88
Fax (356) 67 67 99
E-mail: gwirth@usa.net

NORGE

Swets Blackwell AS

Hans Nielsen Hauges gt. 39
Boks 4901 Nydalen
N-0423 Oslo
Tel. (47) 23 40 00 00
Fax (47) 23 40 00 01
E-mail: info@no.swetsblackwell.com
URL: http://www.swetsblackwell.com.no

POLSKA

Ars Polona

Krakowskie Przedmiescie 7
Skr. pocztowa 1001
PL-00-950 Warszawa
Tel. (48-22) 826 12 01
Fax (48-22) 826 62 40
E-mail: books119@arspolona.com.pl

ROMÂNIA

Euromedia

Str.Dionisie Lupu nr. 65, sector 1
RO-70184 Bucuresti
Tel. (40-1) 315 44 03
Fax (40-1) 312 96 46
E-mail: euromedia@mailcity.com

SLOVAKIA

Centrum VTI SR

Nám. Slobody, 19
SK-81223 Bratislava
Tel. (421-7) 54 41 83 64
Fax (421-7) 54 41 83 64
E-mail: europ@tbb1.sltk.stuba.sk
URL: http://www.sltk.stuba.sk

SLOVENIJA

GV Zalozba

Dunajska cesta 5
SLO-1000 Ljubljana
Tel. (386) 613 09 1804
Fax (386) 613 09 1805
E-mail: europ@gvestnik.si
URL: http://www.gvzalozba.si

TÜRKIYE

Dünya Infotel AS

100, Yil Mahallessi 34440
TR-80050 Bagcilar-Istanbul
Tel. (90-212) 629 46 89
Fax (90-212) 629 46 27
E-mail: aktuel.info@dunya.com

ARGENTINA

World Publications SA

Av. Cordoba 1877
C1120 AAA Buenos Aires
Tel. (54-11) 48 15 81 56
Fax (54-11) 48 15 81 56
E-mail: wpbooks@infovia.com.ar
URL: http://www.wpbooks.com.ar

AUSTRALIA

Hunter Publications

PO Box 404
Abbotsford, Victoria 3067
Tel. (61-3) 94 17 53 61
Fax (61-3) 94 19 71 54
E-mail: jpdavies@ozemail.com.au

BRESIL

Livraria Camões

Rua Bittencourt da Silva, 12 C
CEP
20043-900 Rio de Janeiro
Tel. (55-21) 262 47 76
Fax (55-21) 262 47 76
E-mail: livraria.camoes@incm.com.br
URL: http://www.incm.com.br

CANADA

Les éditions La Liberté Inc.

3020, chemin Sainte-Foy
Sainte-Foy, Québec G1X 3V6
Tel. (1-418) 658 37 63
Fax (1-800) 567 54 49
E-mail: liberte@mediom.qc.ca

Renouf Publishing Co. Ltd

5369 Chemin Canotek Road, Unit 1
Ottawa, Ontario K1J 9J3
Tel. (1-613) 745 26 65
Fax (1-613) 745 76 60
E-mail: order.dept@renoufbooks.com
URL: http://www.renoufbooks.com

EGYPT

The Middle East Observer

41 Sherif Street
Cairo
Tel. (20-2) 392 69 19
Fax (20-2) 393 97 32
E-mail: inquiry@meobserver.com
URL: http://www.meobserver.com.eg

MALAYSIA

EBIC Malaysia

Suite 45.02, Level 45
Plaza MBf (Letter Box 45)
8 Jalan Yap Kwan Seng
50450 Kuala Lumpur
Tel. (60-3) 21 62 92 98
Fax (60-3) 21 62 61 98
E-mail: ebic@tm.net.my

MÉXICO

Mundi Prensa México, SA de CV

Río Pánuco, 141
Colonia Cuauhtémoc
MX-06500 México, DF
Tel. (52-5) 533 56 58
Fax (52-5) 514 67 99
E-mail: 101545.2361@compuserve.com

SOUTH AFRICA

Eurochamber of Commerce in South Africa

PO Box 781738
2146 Sandton
Tel. (27-11) 884 39 52
Fax (27-11) 883 55 73
E-mail: info@eurochamber.co.za

SOUTH KOREA

**The European Union Chamber of
Commerce in Korea**

5th FI, The Shilla Hotel
202, Jangchung-dong 2 Ga, Chung-ku
Seoul 100-392
Tel. (82-2) 22 53-5631/4
Fax (82-2) 22 53-5635/6
E-mail: eucck@eucck.org
URL: http://www.eucck.org

SRI LANKA

EBIC Sri Lanka

Trans Asia Hotel
115 Sir Chittampalam
A. Gardiner Mawatha
Colombo 2
Tel. (94-1) 074 71 50 78
Fax (94-1) 44 87 79
E-mail: ebicsl@slnet.ik

T'AI-WAN

Tycoon Information Inc

PO Box 81-466
105 Taipei
Tel. (886-2) 87 12 88 86
Fax (886-2) 87 12 47 47
E-mail: euitupe@ms21.hinet.net

UNITED STATES OF AMERICA

Bernan Associates

4611-F Assembly Drive
Lanham MD 20706-4391
Tel. (1-800) 274 44 47 (toll free telephone)
Fax (1-800) 865 34 50 (toll free fax)
E-mail: query@bernan.com
URL: http://www.bernan.com

ANDERE LÄNDER
OTHER COUNTRIES
AUTRES PAYS

Bitte wenden Sie sich an ein Büro Ihrer Wahl/Please contact the sales office of your choice/Veuillez vous adresser au bureau de vente de votre choix

Office for Official Publications of the European Communities
2, rue Mercier
L-2985 Luxembourg
Tel. (352) 29 29-42455
Fax (352) 29 29-42758
E-mail: info-info-opoce@cec.eu.int
URL: publications.eu.int

2/2002

15

KK-44-02-464-EN-C

OFFICE FOR OFFICIAL PUBLICATIONS
OF THE EUROPEAN COMMUNITIES

L-2985 Luxembourg

ISBN 92-894-3836-3