



European Commission



Information Society

Le attività di Ricerca e Sviluppo della Commissione Europea nel dominio della sicurezza delle reti e delle infrastrutture

Andrea SERVIDA
Head of Sector

European Commission
DG Information Society - Unit D/4
Trust and Security
andrea.servida@cec.eu.int



OUTLINE



- Why do we need to act **NOW** on security in Europe
- Ambient Intelligence & security
- Towards a European integrated approach to security
- The role of the Commission
- The Commission' support to security standards
- eEurope 2005
- European R&D: from FP5 to FP6
- The international Co-operation



Why do we need to act NOW on security in Europe



- 75% of European companies had no security strategy in 2002.
- In 2002, IT security investments in Europe touched 5 billion dollars (up 25% compared to 2001), i.e. only 1.8% of the overall IT investments.
- 18% of companies spent less than 1% in IT security.
- 10% of companies have just 1 person in charge of security and 45% have between 2 to 5 people.
- 50% of European companies identified the “underestimation of core business risks” as the major obstacle for investments in IT security.
- Security is not strategic yet for 2 companies out of 3.

Source: IDC/Bull survey conducted in 2002 with IT Division of 250 European companies with more than 1000 employees. Over 1000 companies were contacted

In such a situation, there is an urgent need for a collective effort to develop a “culture of security” in the EU



The future: *Ambient intelligence*

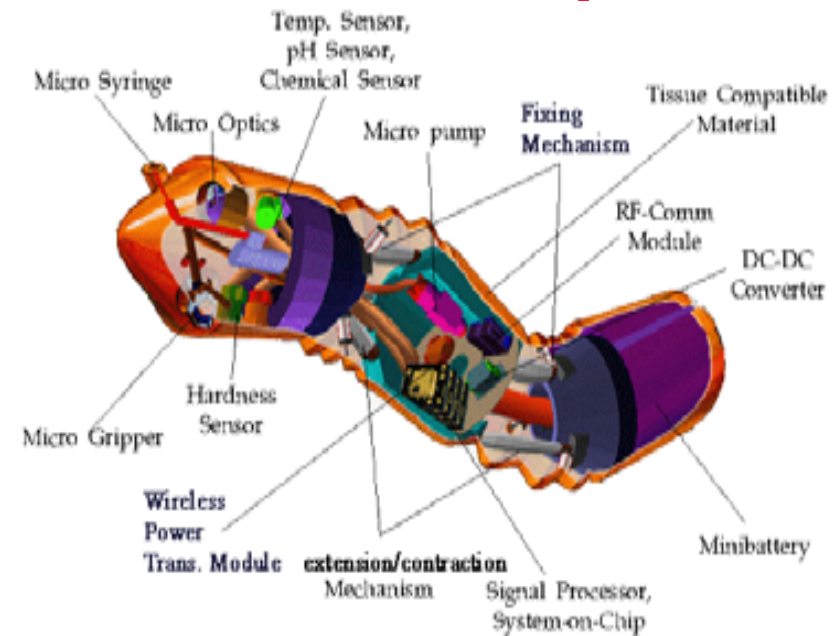


Around us ...

Micro-capsule



Products and equipment at the service of individuals



... inside us ?



Changing the paradigm for security





Why an integrated approach to security in Information Society



- ICT and applications are more and more pervasive to Society, leading to new types of and larger scale vulnerabilities
- Economic and Societal interests go beyond technical security, as they relate to
 - **business opportunities and growth**: new business models, virtual enterprising, delocalised workforces, tailored services, digital asset management, economic value of knowledge, etc.
 - **individual**: privacy, confidentiality, intimacy, cyber-crime, protection of minors, ethics, etc.
 - **society**: new dependencies on volatile technologies, long lasting preservation of knowledge and culture, digital divide, etc.
 - **governments' recognition and power**: interdependencies, critical infrastructures, national defence, social order, international governance, etc.



Why an integrated approach to security in Information Society (2)



- **More and more intelligence and autonomy go in components/systems at lower and lower scale**
 - large scale systems of casually networked and evolving embedded devices,
 - mobile codes in heterogeneous and mobile environments,
 - volatility of networks and service infrastructures
- **Security issues in the digital environment are global**
 - geographical and jurisdictional boundaries disappeared
 - the ultimate basis for “trust” and the recognition of “powers” in the digital environments are changing - recognition of states is blurring, new and local “trusted third parties” emerge, etc.
 - easy, uncontrolled and unlimited access to potentially harmful technologies.
 - the scale of potential disruptions is global



The role of the European Commission



- **Proposes and/or orchestrates the development of the regulatory framework**
 - **Electronic Signature Directive (1999/93/EC)**
 - **Directive on Data protection in electronic communications (2002/58/EC)**
 - **Council Resolution on Information & network security (COM(2001) 298 final)**
 - **Council Resolution on EU approach to a culture of security (2003/C 48/01)**
 - **Proposal for a regulation establishing the European network and information agency (COM(2003) 63 final)**
 - **Proposal for a Framework Decision on attacks against information systems (COM(2001) 521 final)**
- **Launches policy initiatives**
 - **eEurope 2005, e-SAP**
 - **preparatory action on external security/defence**
 - **RTD**



Why is RTD important for policy-making on security



ERA: European Research Area

FP6, Eureka, COST, National RTD Programmes

... towards a Single Market for Research

Lisbon Strategy



"EU: Largest knowledge-based economy by 2010"

Enlargement

The candidate countries are full partners in FP5.

eEurope

Broadband access, e-business, e-government, **security**, skills, e-health, ...

Other policies

Single Market, Single Currency, Security of Europeans, Sustainable Development, ...



Towards a European integrated approach to security



International co-operation

- OECD, G8, Council of Europe, UN, ITU, ...

Economic, business and social aspects of security in Information Society

- Electronic Signature
- Data protection in elect. com.
- Network & information security
- Culture of security
- ENISA
- digital right management, biometrics, smart card, IPv6, open source software
- critical infrastructure protection

Cyber-crime, Homeland security

- Framework Decision on attacks against information systems
- Lawful interception
- G8 CIP
- e-identification/e-authentication
- biometrics in visas and residence permit

External Security/Defence

Preparation action security research

- Pilot action with DGRTD
- Dual use technology research
- Crisis management

Information and Communication Technology - RTD -

- network security, dependability, cryptography, biometrics, identity management, watermarking, ...

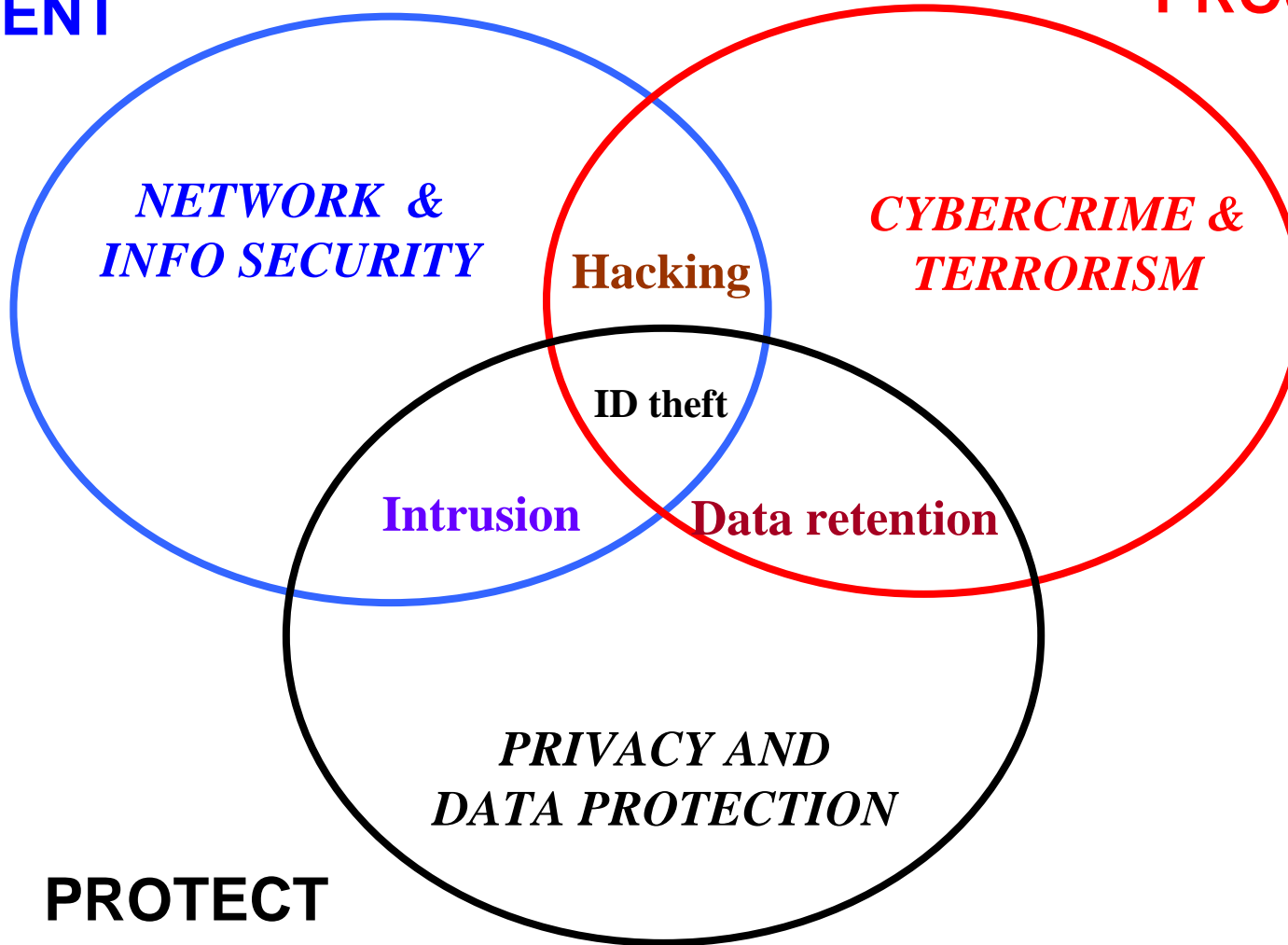


Three angles for an integrated security policy



PREVENT

PROSECUTE



PROTECT



The Commission' support to security standards (CC)



- **Policy level (early '90)**
 - INFOSEC activity led to the publication of ITSEC ('91), ITSEM ('93) and the adoption of the Council Recommendation 95/144/EC on ITSEC;
 - support to the Common Criteria European Team;
 - the Mutual Recognition Agreement ('98).
- **Technical and standardisation activity (late '90)**
 - eEurope 2002: Smart Card Charter - Trailblazer 3 for Smart card;
 - EESSI work for electronic signature - PP for cryptographic module for CSP signing operation.
- **Research and development**
 - FP5 projects.

—————→ ***network and information security***



Communication on Network and Information Security



- Stockholm conclusions (23/24 March 2001) call for the development of a ***comprehensive strategy on security of electronic networks***
...
- In response to this request the Commission adopted the Communication on Network and Information Security on 6 June 2001 - COM(2001) 298



Proposed actions



- **Standardisation and certification (Commission)**
 - accelerate the work on interoperable/secure products and services
 - Commission will support the use of ES
 - MS should **promote certification and accreditation procedures on standards that favour mutual recognition**
- **Awareness raising (MS)**
 - *information and education campaign*
 - *promotion of **security best practice**, in particular to SMEs*
 - *more emphasis on security in education systems.*
- **Security in government use (MS)**
 - incorporate effective and interoperable information **security solutions in e-procurement** activities
 - introduce ES in on-line public services
- Others: European Warning Information System; Technology support (FP6, strong encryption); Legal framework (encryption products and cyber crime); International co-operation



The Council - 1



Council Resolution of 28/01/2002 on a common approach and specific actions in the area of network and information security - (2002/C 43/02)

asks Member States

- to promote the use of the common criteria standard (ISO 15408) and to **facilitate mutual recognition** of related certificates.

welcomes the intention of the Commission

- by the end of 2002 to **propose adequate measures** to promote ISO 15408 (Common Criteria) standard, to facilitate **mutual recognition of certificates**, and to **improve the process by which products are evaluated**, i.e. by developing adequate protection profiles.



The Council - 2



Council Resolution of 18/02/2003 on a European approach towards a culture of network and information security (2003/C 48/01)

invites Member States

- encourage co-operation and partnerships between academia and enterprises to provide **secure technologies and services and to encourage development of recognised standards.**

welcomes the intention of the Commission

- further develop, in co-operation with MS, a dialogue with industry to **improve security in the development of hardware and software products** and ensure availability of services and data



Some open issues



- poor awareness and understanding of security certification needs and benefits
- heterogeneity of testing and evaluation procedures
- duration and costs of certification process
- lack of good and shared practices on evaluation
- mutual recognition of certificates
- limited number of accredited certification labs in the EU, which calls for networking
- workable framework for certification of complex and evolving systems
- emergence of new technologies with specific needs (like biometrics)
- ...

—————→ *...and the future will be more challenging*



eEurope 2005: Secure Information Infrastructure



- **Establish a Cyber Security Task Force - *by mid 2003***
 - supported by Member States and Industry
 - centre of competence on security issues

COM(2003) 63 final “Proposal for a Regulation of the EP and of the Council establishing the European Network and Information Security Agency”
- **Develop a ‘culture of security’ - end of 2005**
 - develop good practice and standards
 - report on progress issued end 2003
- **Secure communications between public services**



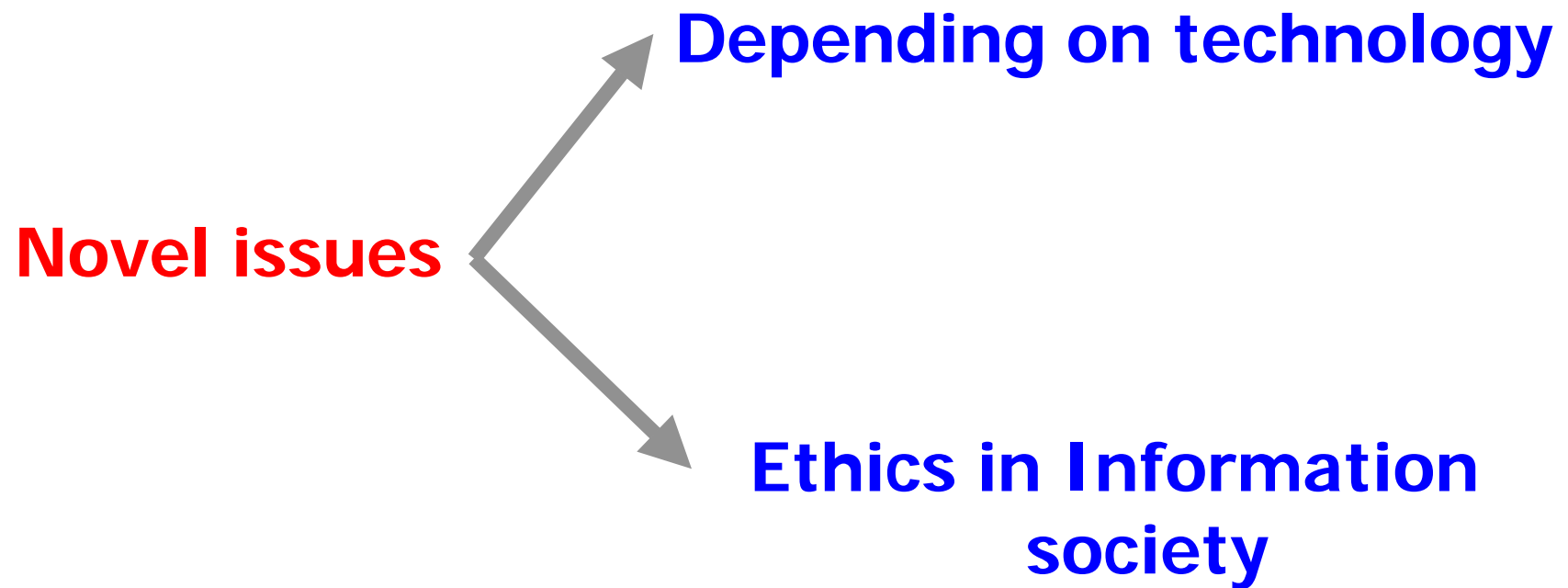
Towards a European integrated approach to security: RTD



International co-operation		
Economic, business and social aspects of security in Information Society <i>- 1st Pillar -</i>	Cyber-crime, Homeland security <i>- 3rd Pillar -</i>	External Security/Defence <hr/> Preparation action security research <hr/> <i>- 2nd & 3rd Pillar -</i>
<i>Information and Communication Technology - RTD -</i>		



Security issues in Ambient Intelligence





Depending on technology



Today issues

Pervasiveness, interdependencies and intrusiveness

Influencing factors

- **Little attention to compatibility between** technology and human systems
- **Little thinking in terms of** privacy respecting Society
- **Little co-ordinated effort to address** dependability of **information and communication infrastructures**
- **Unforeseeable R&D development**

Future objectives

Develop a “respectful”, **productive, innovative and secure IS**

How to go about it

- **Foster a global dialogue on an IS respecting** the personal sphere, safeguarding resilience **of systems & infrastructures**, encouraging innovation, **enabling productivity**
- **Promote the** understanding of interdependencies
- **Share vision on** how to depend on technology
- **Innovative R&D**



Today issues

Poor understanding and awareness of risks to privacy

Influencing factors

- **Globalisation**
- Growing **interconnectedness**
- Increasing **educated consumer**
- Growing **business interest** on **knowing more** about customers
- Increasing use of **digital identities, virtual persona**, etc.
- **Inefficient enforceability** of privacy law

Future objectives

Ethics of privacy as a key element of the **Information Society**

How to go about it

- Make privacy part of **education, training** and **public debate**.
- Socioeconomic research **into privacy** in the Information Society.
- Privacy compatible **processes, products and systems**.
- Build-in **privacy enhancing** mechanisms to **ease enforceability**
- Innovative R&D to **ensure personal control of privacy**.



FP6: between continuity and novelty

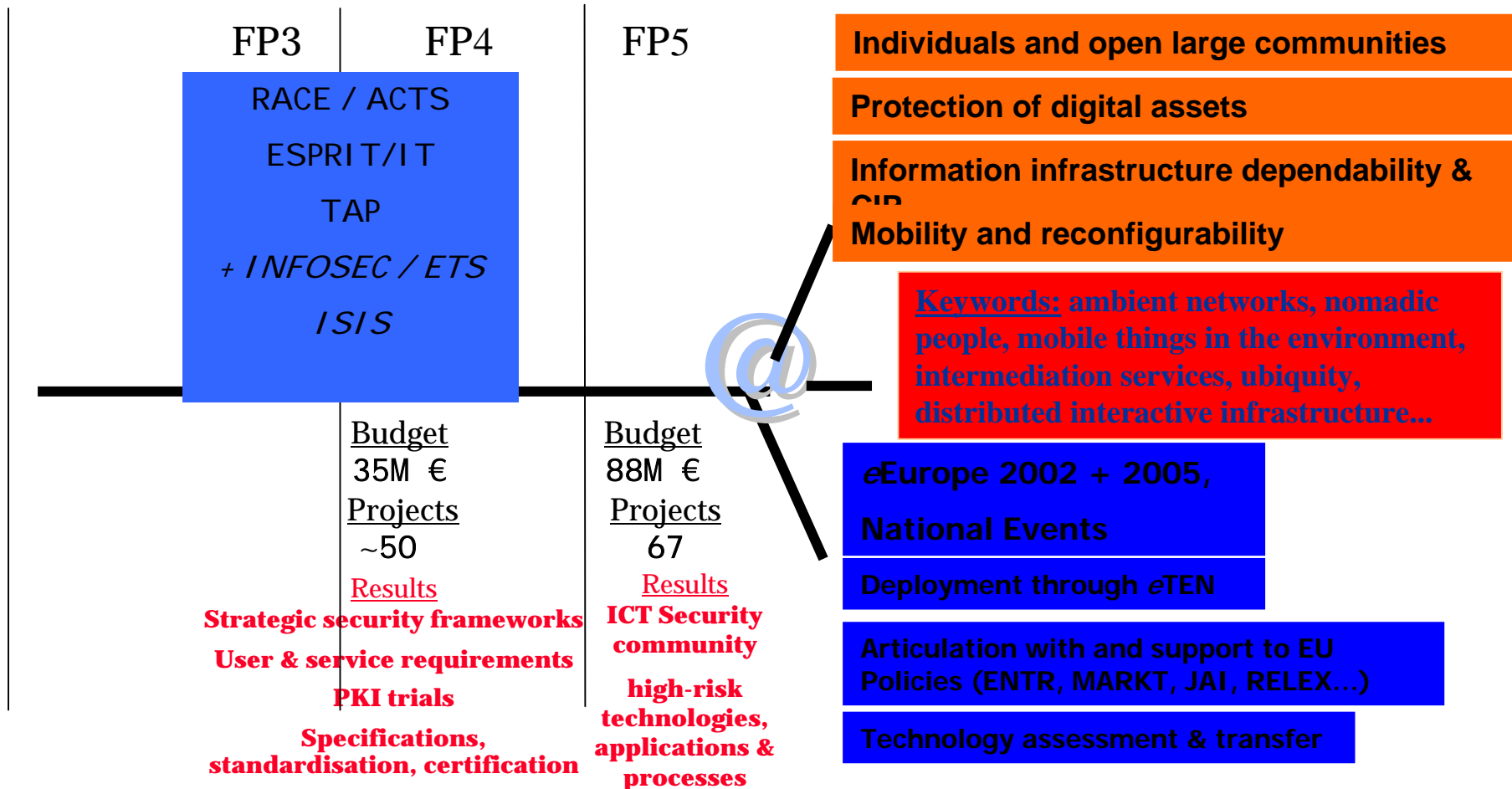


PAST 10 years (1992-2002)

NEXT 10 years (2003-2014)

From Security of Information Systems...

...to Security in Ambient Intelligent Space





IST Priority Call 1:

2.3.1.5 Towards a global dependability and security framework



- **Key Objectives & Breakthroughs**

- security and dependability of ICT infrastructures
- trust and confidence in the use of IST

55 M Euro



- **Research Focus**

- security and mobility, virtual identity management, privacy enhancing technologies
- dependable network and information systems
- simulation-based management decision support tools for critical infrastructure protection
- crypto technologies, digital assets management
- smart devices, biometrics, security certification,...

Closed on 24 APRIL 2003



Building on Call 1 - S.O. 2.3.1.5



- **89 proposals** - 21 IP, 9 NoE, 51 STREP, 8 Other.
- **Provisional results**
 - **7 IPs** on secure IPv6, secure personal devices, identity management, quantum crypto, biometrics, secure justice and secure travel documents;
 - **2 NoEs** on advanced crypto and identity management;
 - **7 STREPs** on secure justice, policy-based network protections, digital passport, smart cards, trust relations, biometrics and CIP.
- **Overall budget of ~76M€**



Towards a European integrated approach to security : Intern. Co-op.



International co-operation		
Economic, business and social aspects of security in Information Society <i>- 1st Pillar -</i>	Cyber-crime, Homeland security <i>- 3rd Pillar -</i>	External Security/Defence <hr/> Preparation action security research <hr/> <i>- 2nd & 3rd Pillar -</i>
Information and Communication Technology - RTD -		



EU-US co-operation on R&D



- **FP6 as the framework for EU/US partnership on R&D**
 - detailed Joint R&D agenda to be drafted (Workshop in Leesburg in Sept 2002):
 - **information assurance and survivability**
 - **secure networked embedded systems**
 - **modelling and simulation of critical interdependent systems**
 - contacts with funding agencies established
 - co-ordination with State Department and OSTP
- **Leverage the EU roadmap projects to develop a joint R&D agenda**
 - a Workshop is being planned
 - investigate the needs and options for joint teams on dependability of global critical infrastructures



EU-US co-operation on R&D - 2



- **US proposal for an initiative on “Perspectives on the Future of Science and technologies”**
 - develop common scientific understanding of future policy issues (among which is **cyber security**)
 - provide policy makers with description of foreseeable development in S&T
 - identify future research needs and opportunities for joint collaboration
- **Co-operation would contribute to raise awareness on global security and dependability challenges**
 - more knowledge and technology
 - wider involvement of stake holders
 - more proactive attitude to secure our infrastructures



WEB sites



www.cordis.lu
www.cordis.lu/ist
www.cordis.lu/rtd2002



IST helpdesk
Fax : +32 2 296 83 88
E-Mail : ist@cec.eu.int

Instruments: <http://www.cordis.lu/rtd2002/fp-activities/instruments.htm>
EoI: <http://www.cordis.lu/fp6/eoi-instruments/>

IRG Workshop on T&S <http://www.cordis.lu/ist/events/workshops.htm>
ISTAG papers: ftp://ftp.cordis.lu/pub/ist/docs/istag_kk4402464encfull.pdf
Roadmap projects: <http://www.cordis.lu/ist/ka2/rmapsecurity.html>
T&S Workshops: <http://www.cordis.lu/ist/ka2/rptspolicyconf.htm>