Privacy standardisation developments in ETSI

Privacy in RFID and ITS

ISO Privacy Standards Conference

Scott CADZOW
Representing ETSI

Contents

- □ **The regulatory framework**
  - ➢ Privacy
  - ➢ Data Protection
  - ➢ Security support
- □ **Modelling for privacy protection**
  - ➢ Ontology
- □ **Specific topic areas**
  - ➢ RFID and EU Standardisation Mandate 436
  - ➢ Intelligent Transport Systems

Privacy, data protection and security

- ❑ **Privacy is a fundamental right**
  - **Article 12 UDHR:**
    - **No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks**
  - **Article 8 EU Convention for the Protection of Human Rights and Fundamental Freedoms: Right to respect for private and family life**
    - **Everyone has the right to respect for his private and family life, his home and his correspondence.**
    - **There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.**

Privacy, data protection and security

- ❑ Assigns rights to citizens on how data related to them is protected
    - ➢ Enshrined in law in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
    - ➢ Supplemented by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Privacy, data protection and security

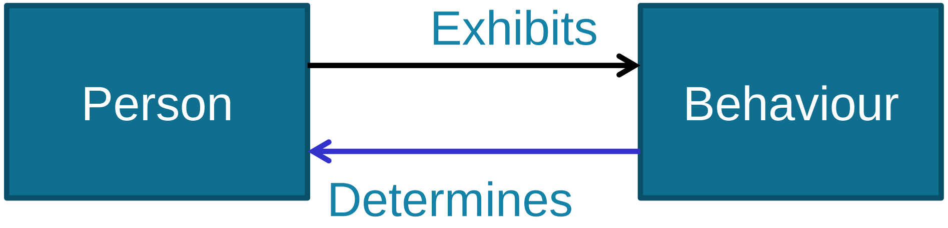
- ❑ **Personal data**
  - ➢ shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- ❑ **Processing of personal data**
  - ➢ shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction
- ❑ **“data subject’s” consent**
  - ➢ shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed

Privacy, data protection and security

- **The means to give assurance of the confidentiality, integrity and availability of data and services**
  - **Offers technical and procedural means to support regulation**

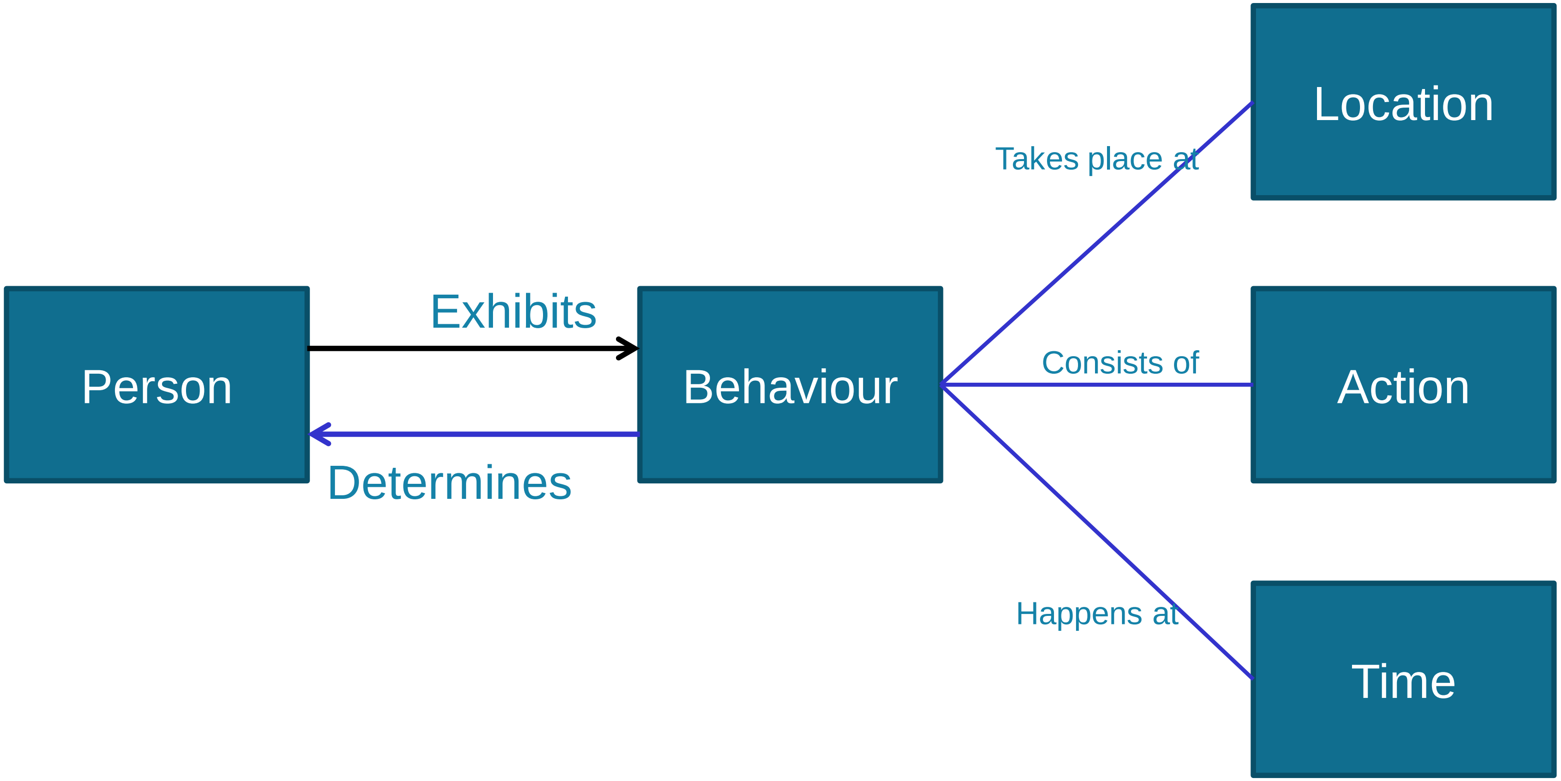
- **Security supports …**
  - **Privacy (Privacy Enhancing Technologies)**
    - **COM(2007) 228 final: “COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on Promoting Data Protection by Privacy Enhancing Technologies (PETs)”**
  - **Data protection**

Attempting to model privacy



The simplest expression of the definition of personal data and the attempt to express it for both the direct and indirect cases.

Wider concept


Person

Exhibits

Determines

Behaviour

Takes place at

Consists of

Happens at

Location

Action

Time

For the wider picture

- Examination of behaviour by itself may reveal personal data without needing to carry explicit “personal” data
- Behaviour is visible in many parts of the telecommunications environment:
  - Protocol stack offers data
    - Time, location (on the network)
  - Application offers data
    - Action (may also give time and location (geographic))

Using RFID as a test case for the Internet of Things

RFID – AN EXAMPLE

EU Mandate 436

- The Mandate addresses data protection, privacy and information security aspects of RFID. It complements the existing legal framework but does not substitute it.
- The objective of the first phase is to prepare a complete framework for the development of future RFID standards.
  - Assumes that there is no existing framework, or if there is that it is deficient

Structure of ESO/STF response

- 1 technical report
  - ETSI TISPAN Work item DTR-07044
  - Analysis and justification for recommendations
  - Recommendations for phase 2 – new standards and gap closure
- Open consultation with stakeholders
  - Other impacted standards groups
  - User and consumer groups
  - Privacy interest groups
- Coordination by group formed from the 3 ESOs

Technical structure of response

- RFID system architecture
  - Taxonomy of terms
  - Ontology of RFID
    - With respect to security
    - With respect to privacy protection
- Consumer, DPP and Security objectives
- Environmental aspects of RFID tags and components
  - RFID hardware end of life considerations
  - Data end of life considerations
- Privacy Impact Assessment outline
  - Role of PIAs
  - Generic versus industry specific PIAs
  - Recommendations for RFID industry specific PIAs
- RFID logos and signage
  - For consumer awareness
  - For device marking

Analysis

- Derived requirements from analysis
  - RFID Logos and signage recommendations
- Standards roadmap
  - Available standards
  - Gap analysis and recommendations

Requirements

Intelligent Transport and its reaction to the privacy debate

ITS – AN EXAMPLE

Consequences for ITS

- ITS carries personal data both directly and indirectly in all its variants:
  - Advanced Traveller Information Systems (ATIS)
    - Location and route is personal information
  - Advanced Traffic Management Systems (ATMS)
    - Who is travelling where, when
  - ITS-Enabled Transportation Pricing Systems
    - Concessionary fares require exchange of personal data
  - Vehicle-to-Infrastructure Integration (VII)
    - CAM and DNM
  - Vehicle-to-Vehicle Integration (V2V)
    - CAM and DNM

How is consent managed in ITS?

- Definition:
  - any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed
- Problem:
  - Correspondents (data transmitters and receivers for CAM/DNM) are unknown to each other
  - Consent cannot be given for general case (it has to be specific)
  - How does the ITS-S user signify his agreement?

Personal data in ITS?

- ❑ Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity
- ❑ Direct:
  - ➢ Restrict transmission of any data that can directly identify a person (i.e. name, address)
    - Unless between known parties who have explicitly consented (with proof) of their willingness to restrict use of the data to explicit purposes
    - Unless such data is protected from eavesdropping and interception
- ❑ Indirect:
  - ➢ Restrict ability of a receiver of data to process data such that it can be linked to a real person

Privacy approaches in ITS

- Shared with the Common Criteria approach
  - Pseudonymity ✓
    - ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use
  - Unlinkability ✓
    - a user may make multiple uses of resources or services without others being able to link these uses together
  - Unobservability 👎
    - a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used
  - Anonymity 👎
    - ensures that a user may use a resource or service without disclosing the user's identity

Views on pseudonymity

- ❑ “ensures that a user may use a resource or service without disclosing its user identity, but can still be accountable for that use”

- ❑ Need to define who/what can make the user accountable
  - ➢ Authority model
  - ➢ Authority enabled against data and services
- ❑ Relies on binding identity to data or service

- ❑ Candidate for RBAC in ITS

Views on unlinkability

- **"a user may make multiple uses of resources or services without others being able to link these uses together"**
- **Key to breaking the link between behaviour and person**
  - **Assumes personal data is not directly exchanged (e.g. pseudonymity)**
- **Techniques to be considered**
  - Allocation of information that describes that an operation occurred can be allocated in several locations within the ITS system such that an attacker does not know which part of the system should be attacked, or the system might distribute the information such that no single part of the system has sufficient information that, if circumvented, the privacy of the user would be compromised – **NOT VIABLE**
  - Broadcast: When information is broadcast (e.g. ethernet, radio), users cannot determine who actually received and used that information – **NOT VIABLE**
  - Cryptographic protection and message padding

What SDOs need to do?

CONCLUSION

Steps we need to take

- ❑ Adoption and formalisation of key approaches
  - ➢ Design for Assurance
  - ➢ Privacy by Design
- ❑ SDOs need to begin to take control
  - ➢ Privacy controls in technology
  - ➢ Privacy controls in management processes
- ❑ The challenge
  - ➢ The need for privacy control is racing against the growing use and development of applications that will introduce new privacy risk.

Who are each of iTour, CEN, CENELEC and ETSI?

BACKGROUND AND CONTEXT

About ETSI

- ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and internet technologies and is officially recognized by the European Commission as a European Standards Organization. ETSI is a not-for-profit organization whose more than 700 ETSI member organizations benefit from direct participation and are drawn from 62 countries worldwide. For more information, please visit: www.etsi.org

About CEN

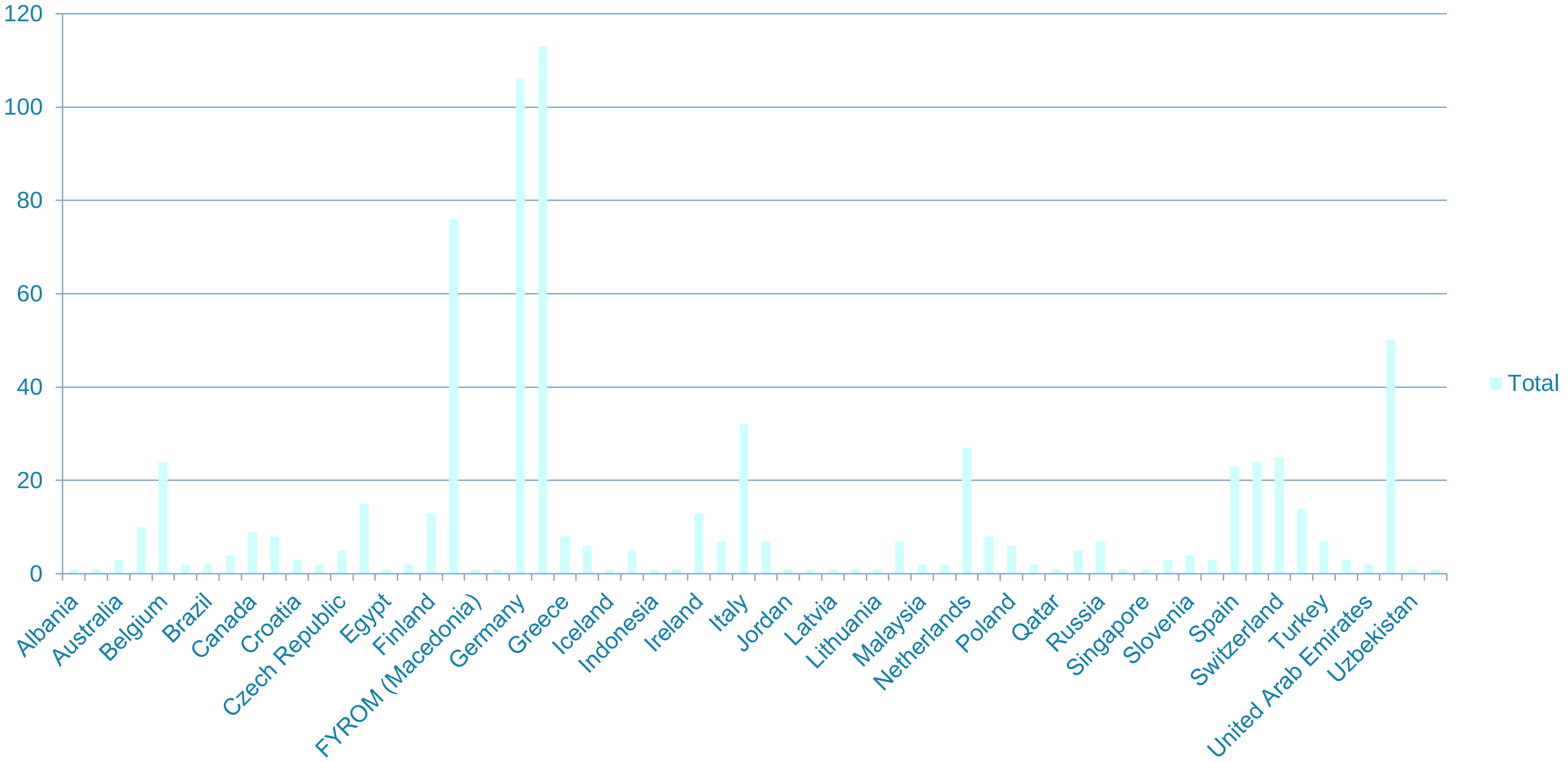
- ❑ CEN is the European Committee on Standardization (www.cen.eu)
- ❑ The CEN members are the 31 *National Standardization Bodies* of the EU, EFTA and Croatia
- ❑ CEN's scope
  - ➢ ~ same scope as ISO, the International Standards Organization
  - ➢ Complementary to scope of ETSI and CENELEC, with of course some areas of mutual interest (an example is RFID)
- ❑ Over 60.000 experts of all fields are active in CEN work (including the work in the national mirror groups)
- ❑ Over 14.000 EN's exist today, with about 1.000 new publications every year
- ❑ Vienna Agreement with ISO – parallel adoption of ENs and International Standards

About CENELEC

- ❑ CENELEC is the European Committee for electrotechnical standardization (www.cenelec.eu)
- ❑ The CENELEC members are the 31 National Committees of the EU, EFTA and Croatia (same geographic spread as CEN)
- ❑ 58 Technical Committees and 14 Sub-Committees
- ❑ 6 500 technical experts
- ❑ > 5 600 CENELEC standards
- ❑ Dresden Agreement with IEC – parallel adoption of ENs and International Standards

- ❑ CEN and CENELEC are supported since 1 January 2010 by a common CEN- CENELEC Management Centre

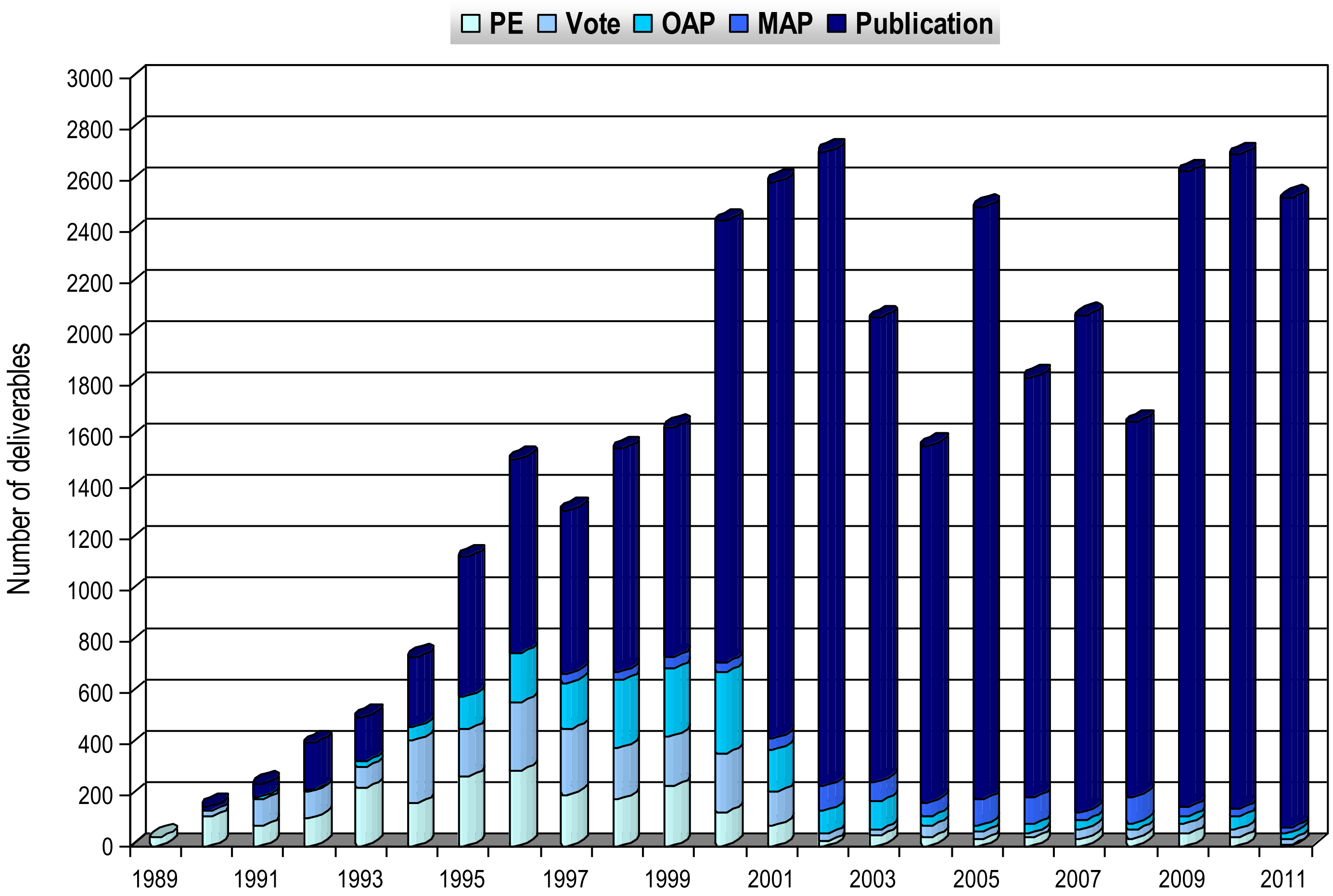
Geographical distribution of ETSI membership



Distribution of ETSI members

ETSI facts & figures

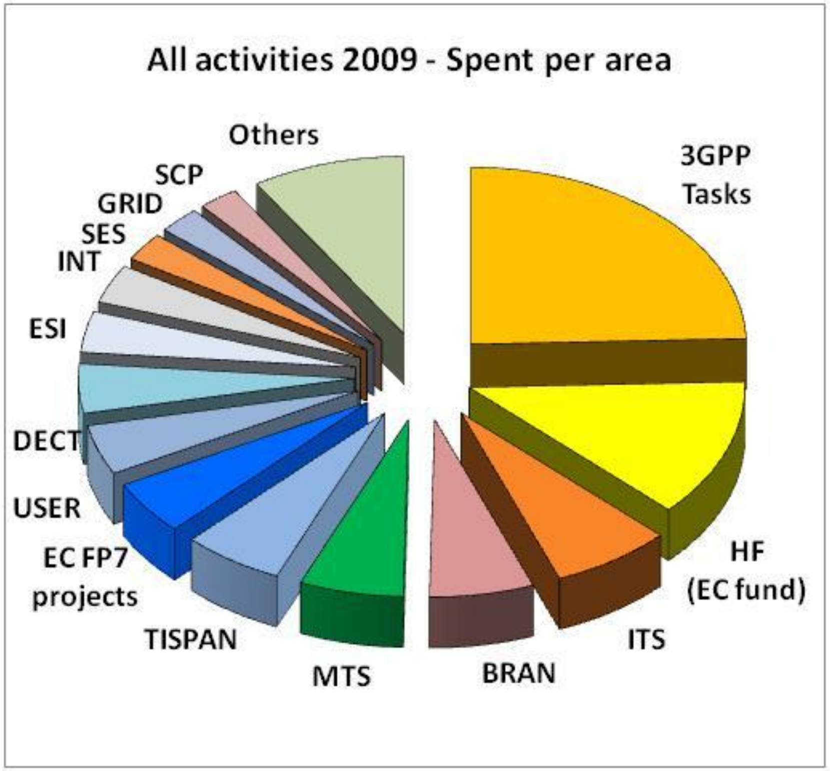
- Standards production (estimate for 2010 and 2011)

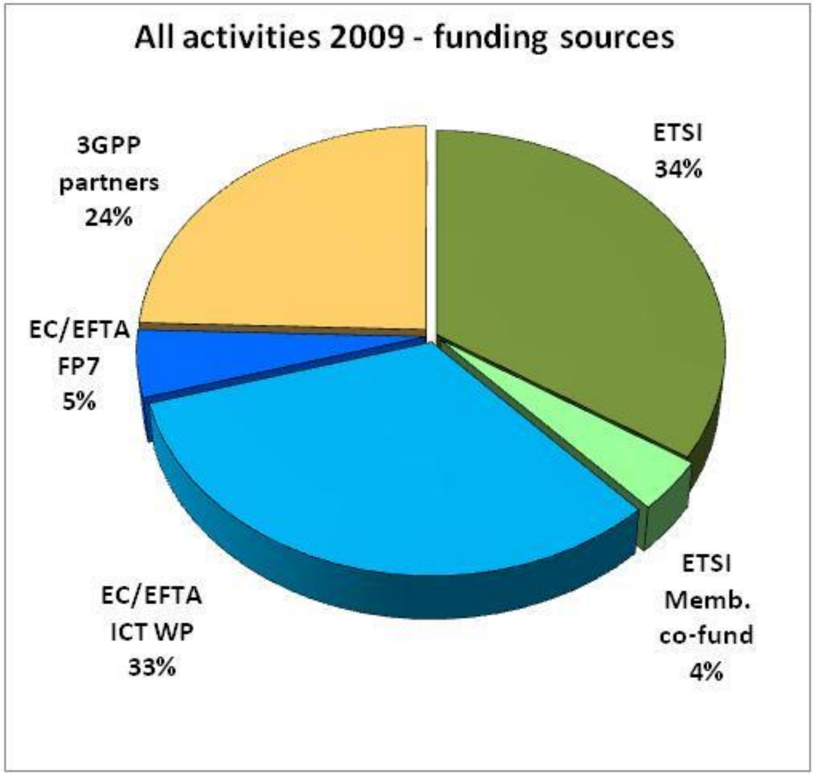


About ETSI Specialist Task Forces (STF)

- STFs are teams of highly-skilled experts working together over a pre-defined period to draft an ETSI standard under the technical guidance of an ETSI Technical Body and with the support of the ETSI Secretariat. The task of the STFs is to accelerate the standardization process in areas of strategic importance and in response to urgent market needs. For more information, please visit: http://portal.etsi.org/stfs/process/home.asp
- The work carried out here is co-financed by the EC/EFTA in response to the EC's ICT Standardisation Work Programme.

ETSI – Specialist Task Forces





iTour

- ❑ **Project aims**
  - ➢ The i-Tour project aims to take the ever evolving services that promote multi-modal transport and offer them to the transport user in a way that allows them to have greater say through their preferences in how the transport options will be supplied to them.
- ❑ **Acknowledgement:**
  - ➢ The research leading to these results has received funding from the European Community’s Seventh Framework Programme (FP7/2007-2013) under the Grant Agreement number 234239. The authors are solely responsible for it and that it does not represent the opinion of the Community and that the Community is not responsible for any use that might be made of information contained therein.