FROM RFID TO THE INTERNET OF THINGS

Pervasive networked systems

Conference organised by DG Information Society and Media,

Networks and Communication Technologies Directorate

6 & 7 March 2006, CCAB, Brussels

Final Report

Prepared by: John Buckley

1 Table of contents

2 Executive summary

- The Internet of Things describes a worldwide network of intercommunicating devices. It characterises the way that information and communication technologies will develop over the next decade or so. It is real concepts that has developed over time and is sufficiently formulated that we can now discuss it and pursue research.

- The concept describes fundamentally worthwhile technology that is capable of supporting the public good, economic growth and personal enrichment of life. It enables pervasiveness of communication technologies in many sectors, with subsequent prospects of ICT based growth and wealth creation through innovation. Example applications of the technology include public disaster management, industrial asset management, and personal lifestyle support.

- The Internet of Things will realise its potential only in the context of a global communications platform that can be used by millions of independent devices co-operating together in large or small combinations, and in shared or separated federations.

- The global platform implies not only a communications resource, but also a set of commonly agreed methods of communicating and operating.

- For reasons of flexibility, adaptability, mobility and survivability, the dominant means of access to and communication within the Internet of Things will be wireless.

- Within the competitive business conditions that prevail today, industry and other players have contributed to an endemic climate of "hype". Economic prospects related to networking of large number of simple devices like RFID are huge. Still, the economic prospects related to more sophisticated computing devices such as sensors need further research with industrial players

- The Internet of things is not a revolutionary concept. It should be understood with an evolutionary perspective, corresponding to the evolution on the networking technologies of today (Internet, wireless, service platforms, etc.). It provides in particular an evolutionary roadmap for mobile and wireless systems.

- Even if evolutionary, a great deal of genuinely creative, innovative research is required to realise the Internet of Things. It is not simply a matter of re-engineering existing technology. Trillions of connected devices are pushing current communication technologies, networks and services approaches to their limits and require new technological investigations. These cannot happen quickly and need to be tackled through a long-term perspective.

- In particular, research is required in the field of Internet architecture evolution, wireless system access architectures, protocols, device technologies, service

oriented architecture able to support dynamically changing environments, security and privacy. Research is also required in the field of dedicated applications integrating these technologies within a complete end-to-end system.

- The issue is considered very seriously in other regions of the world. Japan, Korea and the USA are all considering network and communication technology roadmaps that are related to pervasive networking. Initiatives like GENI in the USA (NSF), and others in Korea and Japan are particularly relevant in that context.

- Recent experience has shown the existence of research of moderate value in this field. Examples include realisations and demonstrations of established technology, or experiments making modest or minimal advances over previous work. Research needs to take a system approach, with cross sector partnerships.

- It is important that researchers when pursuing less constrained, "blue-sky" topics should remain aware of industrial and real-world problems. Industry and academic institutions should be encouraged to keep in close contact, even and especially where the academic research might not attract internal funding within an industrial organisation. Industry should lower and minimise the barriers raised by confidentiality concerns.

- Public entities need to be made aware that the pervasive networking concepts pose new challenges in terms of personal privacy.

- Public entities should carefully check the robustness of their privacy policies and frameworks to the new challenges implied by the emergence of an "Internet of things", where the resulting object identity may eventually be linked to user identity, profiles and consumption habits.

- The Internet of Things is a pervasive federated network in which unregulated personal area and local area networks will interoperate with and through more traditionally regulated electronic communications services.

- Regulators need to carefully monitor the challenges posed by these networks, taking action as necessary to regulate for technical interoperability, consumer protection, support for competition and the appearance of opportunities for the exploitation of market power. Here again, the challenges posed to traditional infrastructure regulatory frameworks should be evaluated.

- A foreseen area where there is risk of monopoly market power is that of the ownership of the data resources in name servers. These are the resources that networks must use to determine the way to reach a given person, device or resource. The implications in terms of Object Name Server (ONS) management should be evaluated.

- Existing regulatory issues that have been and are being tackled in existing, networks, for example access, roaming and billing, may raise their heads in different guises.

- The manner of allocation and regulation of radio spectrum is a key issue for the development of the Internet of Things. Spectrum scarcity will remain an issue and flexible approaches to spectrum management have to be pursued, especially for devices that will primarily be deployed in unlicensed bands.

3 Overview and background

The "Internet of Things" is a network of billions or trillions of machines communicating with one another. It is a major or dominant theme for the evolution of information and communications over the next few decades, and in its simplest form it is already here. There were 1.3 billion radio-frequency identification tags (RFIDs) and two billion mobile service users, worldwide, in 2005. The idea has grown from advanced concepts from the last twenty years:

- ubiquitous communications
- pervasive computing
- ambient intelligence

This concept is not only the result of a technology push. The conference clearly showed that technology push in this field is mirrored by a market pull, with shorter term objectives and tangible application prospects, at least for simple devices such as RFID. The longer term view is pushed by the visible trend towards ever more networked devices, but the economics related to the networking of a myriad of advanced objects with much more advanced computing capabilities require further research. The conference addressed these two perspectives.

From a generic point of view, it can be concluded that the trend towards an ever larger population of connected intelligent objects is irreversible, because the economic value of a system of objects and devices is directly related to the fact that they are "networked". Networking is the real added value.

From the technological perspective, the Internet of Things will enable computing to melt invisibly into the fabric of our business, personal and social environments, supporting our economic, health, community and private lives.

Here are three simple examples.

- Asset management. Electronic tagging and remote sensing tracks the location of baggage in an airport, or of goods in a factory production process
- Healthcare. Blood pressure and heart rate sensors relay regular readings from a patient's home to a monitoring centre. A computer detects adverse movements and signals a doctor to review the patient's case
- Environment monitoring. A network of sensors monitors river heights and rainfall, predicting floods and supporting water management measures for flood relief.

The potential applications of pervasive networking are limitless. Some proposals appear essential, for example people and resource tracking in a disaster scenario such as a tunnel fire. Others may at first sight seem unrealistic. To make this technology really worthwhile, there is a need to address large classes of potential applications in order to better understand the various requirements (e.g. real time, quality of service) that will eventually drive the needed "generic" technology developments.

The Internet of Things is currently a very popular subject. It receives lots of attention from various regions of the world and from diverse research communities. It may even be considered as a field leading to an inflation of research papers whose actual

scientific value may be questionable. Rescuing this topic from a pure hype phenomenon requires a strong industrial drive and a clear industrial commitment implying an application perspective that goes beyond the classical RFID devices.

Much fundamental research remains to be done to make the economic and application promises of pervasive networking happen. "Be not afraid of moving slowly, be afraid of standing still," is a motto that was presented as particularly appropriate in this context.

Application drive alone will not deliver the wide variety of solutions that have to be brought together. Our target network architectures are often conceptual frameworks using devices we cannot yet obtain, assembled with tools we do not yet have. The list of research we need to acquire those tools and materials is a long one that ranges across a range of industrial sectors, beyond the classical telecommunication technology providers.

These technologies also bring us face-to-face with questions about the sort of society we wish to create (for example, the surveillance society). Pervasive technologies are clearly related to problems that go far beyond the purely technological issues, and that need to be addressed by public authorities. The way we conduct effective research in a competitive environment is another issue that emerged for a field which is particularly complex, as it ranges from the device/component to the system, network and service architecture.

In the opening of the conference, the issues considered as being of relevance were introduced as being:

- The system perspective, how networked systems are likely to evolve.
- The implications of device connectivity on future network architectures and technologies.
- The specific security, privacy, trust and confidence issues.
- The service architectures that are needed to support the applications of trillions of connected devices.
- The service composition and delivery prospects.
- The role of "open" (software) models.
- The role of wireless technologies.
- The related non R&D issues, such as governance, spectrum and consumer acceptability.
- The developments in other regions of the world and prospects for collaboration.

These were introduced as questions to be answered in order to understand the requirements for the global network of tomorrow, how it can be built and what it should look like.

This report aims to analyse and summarise the presentations, discussions and conclusions on these various issues.

4 System perspective

The Internet of Things is a network of communicating devices. Devices have four degrees of sophistication. The final stage makes "**Proactive Computing**"[1] possible. These devices, aware of their context in the physical world, react to that context with some form of action. This may respond to the context and cause the context to change.

- Purely passive devices (RFIDs) that give out a fixed piece of data when remotely queried.
- Devices with moderate processing power to format the message and maybe vary it with time and place.
- Sensing devices that generate and send information about their surroundings, for example pressure, temperature, light level, location.
- Devices with more processing power that can decide, without human intervention or without needing first to be being queried, to communicate with another device.

The power of the Internet of Things and the applications it supports arises because devices are **interconnected**. Devices in the Internet of Things are sometimes called "Smart Devices", though groups of devices need not be equally smart. A **gateway device** may filter, aggregate and format data from a group of simple sensors before sending it somewhere else. This issue is in particular related to wireless access and architecture choices, which may vary as a function of the application requirements.

Radio communication is vital to the Internet of Things. Firstly and obviously, it supports ubiquity and mobility. Devices can move and go anywhere. Secondly, it supports a flexibility that would be impossible with wired communication. A device can move into a group and then move out of it again. New devices can join an existing group, so increasing the number and power of the things that the group can do collectively.

The Internet of Things calls for a new class of network, introduced as **Capillary Networks**[2]. These short-distance, edge networks extend existing networks and services to all devices equipped with sensors and actuators and the physical environment in general.

Different device requirements clearly emerge, driving different architectural choices: devices may need to communicate with one another at any distance, and different communication media and technologies are appropriate for the following categories.

- A few cm (Body Area Network, BAN)
- A few m (Personal Area Network, PAN)
- 10's or 100's m (Local Area Network, LAN)
- A few km (Metropolitan Area Network, MAN)
- 10's or 100's km (Wide Area Network, WAN)

[1] This terminology was introduced by Intel as a conceptual driver.
[2] Terminology introduced by France Telecom to illustrate how pervasiveness may be achieved.

- 1000's km (Global Area Network)

Long distance communication will most likely continue using a communication service provider, for example a cellular, 3G or fixed network operator as at present. Capillary Networks apply to the BAN, PAN and possibly LAN environments, with gateway devices providing the interface between levels where needed.

Capillary networks will be **autonomous, self-organising mesh networks,** because of flexibility and economy. Small networks cannot bear the cost of configuration, management and maintenance, therefore the Internet of Things will need "arrive and operate" just as we require "plug and play" with wired computers. Neighbouring devices will exchange messages to discover one another and configure for themselves the best topology for exchanging and relaying messages to, from and through one another. In this way, the network can react when a device arrives, leaves or moves, and can keep going when there is interference and disruption to transmission paths. The self-organising, dynamic routeing capability forms a basis for the survivability and dependability of the networks of the Internet of Things.

Service platforms must evolve beyond the current limitation of "static" service configurations and to move towards service oriented architectures. Today, services are rather programmed and do not dynamically adapt to changing application requirements and contexts. Interoperability does still require that client services "know" the features offered by service providers beforehand. This "closed-world" approach implies that all services and service features are known in advance. On the other hand, semantic modelling should make it possible for service requestors to "understand" what service providers have to offer. This is a key issue for moving towards an "open-world" approach where new, unknown or modified devices/services may appear at any time. This has also implications on middleware requirements, as these are needed to interface between the devices, that may be seen as "services", and the application. This is a key issue to progress towards device networks capable of dynamically adapting to context changes as may be imposed by application scenarios (e.g. moving from monitoring mode to alarm mode to alert mode may imply different services and application behaviours).

Devices in the Internet of Things must be able to communicate with any other device anywhere in the world. This implies a **naming and addressing** scheme, and means of **search and discovery**. These will find whether a desired device exists, where it is, and which communications channel is required to reach it. This implies in turn that information provided by these devices may eventually be aggregated and used with more classical information, as found on a traditional web server. The fact that devices may be related to an identity (through naming and addressing) raises in turn a number of privacy and security challenges.

The Internet of Things must conform to **standards and standard methods of operation**. While it might be possible for any individual application to use its own application specific devices, protocols and methods of operation, there are beneficial economies when standard interoperable platforms are readily available.

The Internet of Things must be **reliable and dependable** in the face of device malfunction, abnormal traffic loads and patterns and malicious attack. It should safeguard policies regarding ownership of information and authority to access devices, giving due respect to people's rights of **privacy**.

5 Technology perspective

5.1 Devices

The principal device challenges appear below.

- Size
- Cost
- Powering and energy efficiency
- Sensors
- Device installation
- Special environments

The **size** of existing RFIDs is about:

- 10 cm x 4 cm for 900 MHz operation
- 6 cm x 1 cm for 2.45 GHz operation.

It was reported that Hitachi has an embedded microchip for an RFID that is 0.15 mm square and 7.5 μm thick. Progress with many applications, for example identity cards, banknotes and tagging small items, will depend on size reduction. The truly invisible sensors needed for pervasive networking need more dramatic size reductions. People spoke of grain-sized devices ("smart sand") and even smaller ("smart dust"), though these are aspirations rather than forecasts.

RFID **costs** are in the region of €0.50 for retail product tags and supply chain tracking applications, but rise dramatically beyond €25 for the more sophisticated devices used for example in highway toll collection. The drive for wider application depends on much lower costs. Printed circuitry is a possible approach, and a major driver in practice will be manufacturing scale and volume.

The feasibility of many applications depends on **powering** and **power economy**, yet there are deep challenges here. Devices must have long lifetimes without the need to change batteries. Consumers will not accept goods where the run-down of an active device or the need to buy and fit a new battery dominates the practical lifetime of the item. In other applications, for example environmental monitoring, the cost of access to change batteries might be prohibitive. All devices and applications face the problem of power scavenging, since only with a minority of electrical goods will there be a ready source of power. It was reported under the IST project e-SENSE that an energy efficiency of 20 nJ per transmitted and received bit is a challenging objective, with a current state of the art figure of 50 nJ and the average in the hundreds. While the simplest passive RFIDs do not require power, it is needed for any significant amount of processing.

Sensor technology itself needs to evolve; in many cases, miniaturised sensors require further R&D. In addition, sensors have to be fitted with communication capability and also with service features, to cover the most extensive use cases. These issues are clearly in the R&D domain, as the impact of these communication and service features on the devices are expected to have non-negligible cost impact.

The **placement of tags and sensors** is not always easy, so work is needed to develop ways of making tags adhere stably in some applications. This is especially important if a sensor has to remain in firm contact with the thing it is measuring, such as surface temperature. It was reported that methods of 3D printing, laser sintering and material deposition as techniques of bonding sensors to surfaces may be suitable approaches.

Already, applications are foreseen in **specialised environments** where the normal transmission of radio does not work well. These include underground, coastal and submarine sensors. These issues are in particular explored in the context of US programmes, and are putting specific design constraints on the devices.

5.2 Networking

Networking of devices is a multifaceted issue that has impacts at various layers, at the periphery and within the network. An extensive range of networking issues was presented during the conference.

The main reported challenges are outlined below.

- Network heterogeneity
- Standards
- Lightweight protocols
- Protocol delayering (layers co-design)
- Autonomous self-organising networks and adaptivity
- Network discovery
- Dynamic routeing
- Network survivability and dependability
- Network scalability
- Naming and addressing strategies
- Declarative programming
- Programming platforms and application program interfaces (APIs)
- Traffic and congestion management
- Real time resolution and delay tolerance
- Error detection and correction

Most networking aspects of the Internet of Things are in the domain of research problems. They need high-quality and original thinking, as they are not reapplications of existing solutions. The network requirements described in the "Systems Perspectives" section are currently met only in the most limited ways, if at all.

Networking aspirations may conflict with the physical reality of devices. We would like clever protocols, for example for network self-discovery or to implement system resilience, but find that these call for processing power. At the same time, we want them to run on infinitesimally sized devices that consume no power. This set of conflicting requirements calls for early end-to-end system design and optimisation.

Some key requirements must be designed from the beginning. These include adaptivity, evolvability and (as described in later sections) security and privacy. It is unlikely to be effective to introduce these features as later increments.

The Internet of Things will be a **heterogeneous network**, being made up of federated, heterogeneous networks. It must accommodate devices:

- from different makers
- of different dates and release versions
- of different capabilities and sophistication
- of different speeds
- using different technical interfaces
- converging differing functions

Devices and gateways will have to recognise these differences and mediate where necessary.

Technical standards are essential for an open, evolving platform. Standards are required for:

- intercommunication and interoperation
- sensor and actor co-ordination and communication
- self-organisation and adaptivity
- service description and capability declaration
- routeing and transport methods
- radio interfaces and media access
- localisation and synchronisation
- publication and subscription of devices and resources
- resource management and reservation, and admission control
- security
- encryption (end-to-end and hop-by-hop) and key distribution
- user interfaces

Standards must be extensible, allowing devices to communicate together at the level of their common functionality. Devices should behave predictably when presented with a message they may not understand, while transit devices should pass on end-to-end messages even if they might not understand the entire content.

Existing data communication protocols may be inappropriate in the Internet of Things. Present-day protocols typically need hundreds and more of kilobytes of program code (software) to run them. It was reported that even the simple ZigBee protocol common in RFID applications requires a 48 kb stack, which is overly complex for tiny sensors. The ISO Seven-layer model has conditioned a whole generation of telecommunications and information technology protocols. This approach is now showing its limitations and pervasive networking requires new

approaches. Lighter protocols and lighter implementations that melt down (compress) the explicit protocol layers into a single communications module are now required.

The Internet of Things requires **self-organising networking** to give ready-to-go "arrive and operate", mobility, economy and flexibility as well as network resilience. Self-organising adaptivity is a necessary counterpart of an unpredictable world, and must be addressed from the beginning. Self-discovering and self-organising mesh networks remain a research topic: we must find the key problems, developing methods and protocols that result in optimised or adequately performing networks. Self-organising networks must cope with varying requirements for physical and virtual link topologies. Service discovery and reuse by different applications has very high priority. Different applications may require topologies such as stars, rings or full interconnection, and the requirement may vary with normal, alert, alarm, disaster and other modes of operation.

Dynamic routeing is the ongoing counterpart of self-organisation, where networks re-route themselves after the initial discovery and set up. This might occur when a new device arrived, a better path became available (for example when a mobile node moved nearer to a gateway) or under problem conditions like interference, loss of a device or breakage of a transmission path. Earlier approaches such as Manet for ad-hoc networks have been reported as not fully convincing, and this remains an important subject for research.

The Internet of Things must **scale to potentially very large networks** of many objects and devices. This implies the right design choices. Centralising network knowledge or relying on discovery procedures that require a querying process to access very many other nodes, militates against scalability. Scalability implies distribution of the control plane and of data processing, and these contribute also to survivability and security.

The Internet of Things must have a **naming and addressing strategy** by which objects can identify themselves, and can locate other objects and the communication paths to them. Because the network is heterogeneous, supporting many different devices offering different service types, a **declarative interface**, like IDL or XML, will be needed. This will to allow a device or node to describe what it presents to others.

A consistent set of **middleware** offering **application programming interfaces,** communications and other services to applications will simplify the creation of services and applications. Service approaches need to move from a "static" programmable approach towards a configurable and dynamic composition capability.

The Internet of Things must incorporate **traffic and congestion management.** This will sense and manage information flows, detect overflow conditions and implement resource reservation for time-critical and life-critical data flows. There will be a high research content here, since no one really knows the traffic characteristics of the Internet of Things. It was reported that known traffic asymmetry profiles in today's networks generated by interactive usage over broadband Internet access connections may radically change in the future. It could well happen that in the future, the main network load does not happen "downstream" from the network towards the terminals, but rather upstream from the devices towards the networks. This will in turn call for intelligent strategies at the level of traffic shaping and filtering, and require further processing capabilities at the edge of the network. Edge networking capability is also

expected to be application dependent, as some safety critical applications with real time constraints may not be compatible with the extra latency imposed by such edge network processing.

The networks must support **real time resolution**. For many applications the sequence and timing of messages may matter, yet self-organising networks and packet-based transmission guarantee neither transit time nor even the sequence of received messages.

Finally, the Internet of Things will need **error management**. A graded set of facilities will be necessary to match different application requirements. On the one hand error management adds overhead costs to processing power, data rates, data volumes and transmission time. On the other hand, errors may be of modest concern in some applications and yet life-threatening for others.

5.3 Security and privacy

People will resist the Internet of Things if there is no public confidence in it. The Internet of Things will affect and control events in the real world and will contain information of value. It is bound to attract unwelcome attention. Digital crime is becoming an industry in itself, and criminals are early adopters. Where society places high reliance on a pervasive technological infrastructure, some may want to disrupt it. Public fears are likely to focus on a handful of security and privacy factors.

- Vulnerability to attack
- Tag cloning and identity theft
- Access rights to data
- Quality and integrity
- Capture of personal data
- Retention of personal data

There are various ways to attack the functioning of a network:

- Node destruction
- Transmission impairment or destruction, for example using interfering signals
- Flooding a network with false messages (denial of service attacks)

Resilience is something we can engineer into a network, using the techniques of network engineering. Adequate **security architecture** must be developed at the outset. It is likely to include security and distributed database architectures, and layered network philosophy allowing devices to retreat to trusted links and components when under threat. It is essential to understand and model the detailed nature of potential threats, to be sure that networks are indeed survivable. The following are relevant technical approaches at network level.

- Dynamic routeing
- Error correction
- Traffic management and information flow control
- Dynamic selection of the radio channel

- Diverse routeing
- Redundant provision of devices, nodes and processing resources
- Network design principles for integrity and quality of service
- Security and reliability architecture
- Security and reliability toolbox
- Reliability-aware components

People and things can pretend to be what they are not. For example a counterfeit product may acquire a tag that marks it as genuine; a person may try to acquire another's identity. The conference named this phenomenon **tag cloning**.

One of the presentations described a physical method of creating an unclonable tag, by coating it with an opaque material containing particles of high dielectric constraint. The random pattern of the particles gives the device a "fingerprint" that is difficult or impossible to replicate.

At system level, it was argued that security is better when you have to join things up rather than rely on a single component. It was also indicated that good security depended on a system-oriented view that allowed multiple identities varying over contexts and time. Attempts to create security using a single component, the "unbreakable key", may fail and so do more harm than good. An example is biometric identity data that a person cannot revoke: what if someone found a way of faking it? Some principles for good security were reported as follows.

- Don't have a constant identifier.
- Spread the security over system components.
- Allow multiple forms of the personal identity.
- Vary the required form of identity over time, or by exchanging a message at each access.
- Lock identity data to particular contexts.
- Give people the capability to revoke their identity key.
- Take a risk management view.
- Focus on security, not surveillance.

Privacy is an issue that worries many people. The Internet of Things will collect much data about personal movements, purchases and actions. With the cost of storage below one nano-euro per byte, information can be retained indefinitely. This places the individual in a position of denied oblivion with universal observability. The technical measures to safeguard privacy include:

- ownership of data
- access rights
- ownership of processes
- authorisation for intercommunication and interoperability
- the ability to neutralise a tag ("tag clipping")

- context sensitive tag behaviour

However, technical countermeasures will achieve very little if incentives are misaligned or the real motives are against privacy.

5.4 Radio spectrum aspects

Radio is fundamental to the Internet of Things. It is a flexible network of wirelessly interconnected devices, where "radio provides the magic" that is the "ubiquity capability". It would be severely restricted and might not develop at all if all connections had to be wired. In today's world, there are about two billion mobile phone users and the overall ratio of radios to human beings is one to one. According to an ITU report, we are entering an era where this ratio could exceed 1000 to one. What spectrum these radios will use, and how will it be allocated and managed, are open questions.

This section of the report addresses only technology issues. The section on "Non-research perspectives" deals with policy and regulatory issues.

Efficiency of spectrum usage is seen both as a requirement and a trend**.** Currently the state of the art is in the range one to five bits per second per Hz per cell. A gain of at least a factor of two and maybe an order of magnitude is a common research objective.

The air interface technologies for the Internet of Things, known as **alternative wireless technologies** (AWTs), remain in the main to be developed. Existing technologies are candidates to form the bases for them, including:

- ZigBee (IEEE 802.15.4)
- WiMax (IEEE 802.16)
- WiFi (IEEE 802.11 variants)
- Bluetooth (IEEE 802.15.1)
- UWB (IEEE 802.15.3a)
- Flash OFDM (IEEE 802.20)

Only in the 0.7 – 7 km range, the standard mobile telephony cell, are there as yet clearly established technologies.

It is likely that the Internet of Things, or at least significant parts of it, will use **spread spectrum technologies** in preference to the more traditionally current **single frequency approaches**. Spread spectrum technologies send the signal over a wide frequency band but with very low powers in any one particular band. The signals resemble white noise, except to receivers equipped with the codes to decipher them. The reasons in favour of spread spectrum technologies are as follows.

- They are spectrally more efficient.
- They are less vulnerable to interference than a mono-frequency signal. This could prove critical in environments such as the car.
- They are more adaptable. They can move the energy of the signal into less crowded bands. This gives them more interference tolerance, while simultaneously inflicting less interference on neighbouring users.

The Internet of Things calls for major steps forward in radio technology.

- **Cognitive radio**: the radio senses the transmissions reaching it and the ambient level of interference.
- **Gap finding**: the radio finds the best frequency bands to use.
- **Software defined radio**: a transmitter and receiver is not tied to one frequency, media access control (MAC) protocol and messaging format, but can vary these as defined by a stored data template.
- **Smart antennae**: aerial systems can vary their strength, direction and radiation pattern according to a stored data template.

Advanced radio technologies substitute computer power for simple transmission around one frequency. Sometimes, computer power will be the scarce resource. It seems questionable whether the smallest and cheapest of devices, working on minimal power budgets, can possibly have all or any of these advanced capabilities.

5.5 European IST research projects

Experts from seven currently funded IST research projects presented their views on the conference themes. These projects represented were:

- **PROMISE** (6th Framework, integrated project, 507100) Product lifecycle management and information tracking using smart embedded systems
- **EYES** (5th Framework IST-2001-34734) Energy efficient sensor networks
- **e-SENSE** (6th Framework, integrated project, 027227) Capturing ambient intelligence for mobile communications through wireless sensor networks
- **MAGNET** (6th Framework, integrated project)
- **RUNES** (6th Framework, integrated project, 004536) Reconfigurable ubiquitous networked embedded systems
- **UbiSec&Sens** (6th Framework, specific targeted research project, 506926) Ubiquitous networks with a secure provision of services, access, and content delivery
- **CRUISE** (6th Framework, network of excellence, 027738) Creating ubiquitous intelligent sensing environments

Their contributions are synthesised in the other sections of this report. These projects are addressing various aspects of pervasive networking, such as PAN, BAN, low power sensor architectures and security models. The variety of the presentations highlighted a need to bring these activities under a more systematic and co-ordinated umbrella under FP7.

6 International perspective

6.1 Introduction

Three presentations updated the conference with views on research progress and initiatives in other countries.

- Ian Akyildiz from the Georgia Institute of Technology, on the USA

- Shingo Ohmori, from the National Institute of Information and Communications Technology, on Japan
- Daeyoung Kim, from the Auto-ID Labs Korea Information and Communications University, on Korea

6.2 The USA

The first talk outlined the major research programmes currently being funded by the National Science Foundation (NSF) and the Department of Defense (DoD) of the **USA**. The NSF programmes are:

- The GENI (Global environment for networking investigations)
- FIND (Future internet network design)

GENI deals with:

- new architectures for pervasive computing, mobile, wireless and sensor networks
- building new services and applications
- deployment and validation

FIND addresses architecture, mobile wireless and sensor technologies.

The DoD programmes are:

- Automated wide-area network configuration from high-level specifications
- Robust self-forming human networks: making organizations work
- Modification of WiFi communication devices to support the urban warrior
- Scalable mobile wireless mesh networks
- xG (Dynamic spectrum access). Cognitive radio networks
- CBMANET (Control based mobile ad-hoc networks)

The presentation drew attention to some research papers showing the formidable amount of work needed to address the research challenges. The presentation put emphasis primarily on the network architecture challenges, taking into account various application scenarios. Most of them are reported in section 5.2 above.

It was also indicated that pervasive networking with computing and sensor networks has become a very popular subject, with a huge number of publications over the recent years having diverse scientific value.

6.3 Japan

Japan is a technologically advanced nation with world-leading positions in the cost of broadband internet access and the proportion of internet-enabled mobile phones. It was presented how Japan had launched a government – industry initiative in January 2001, the “e-Japan Strategy” designed to make Japan one of the most advanced IT nations within 5 years. The e-Japan strategy met it its 2005 targets for high-speed enabled homes well before time.

The next step after e-Japan was the UNS of July 2005. UNS stands for "Universal communications, new generation networks, new security and safety for the ubiquitous networked society", and presents the vision of the forthcoming networked society of 2010. UNS combines universal communications and new generation networks with security and safety. Elements of UNS include:

- ubiquitous sensors and RFID
- ubiquitous ad-hoc networks
- universal personal area networks using UWB
- context aware software, recognising the user's intentions
- multi-agent software
- biometric authentication
- proper and efficient handling of copyright of digital contents
- distributed and co-operative functionality
- adaptive context-aware services

Targeted applications include:

- the "ubiquitous home"
- traceability of food
- "Super intelligent urban card", starting at Tokyo railway stations

A short video of the "ubiquitous home" demonstrated a home displaying among other facilities:

- a home robot, following the householder and helping her find things
- automated, sympathetic choice of TV programmes
- checking by RFIDs of the contents of a handbag.

This presentation clearly showed that future home networks and environments are key targets for these technologies.

6.4 Korea

The third speaker presented the Korean u-IT839 strategy. This strategy is a master plan for the IT industry, in an effort to gain more growth momentum from the IT sector in Korea. It aims to promote eight services, build three infrastructures and develop nine growth engines, as an evolution of the former 839 strategy.

The ***eight*** services are:

- 2.3 GHz mobile Internet (WiBro)
- DMB / DTV service
- u-Home service
- Telematics service
- RFID-based service

- W-CDMA service
- IT service
- VoIP service

The ***three*** infrastructures are:

- BcN / IPv6 (Broadband convergence network)
- USN (Ubiquitous sensor network)
- Software Infrastructure

The ***nine*** "growth engines" are:

- New generation mobile phone
- Digital TV
- Home network
- IT SoC
- Post PC
- Embedded software
- Digital contents
- RFID / USN
- Intelligent Robot

The RFID / USN strategy, termed Ubiquitous life (U-life), aims at key technology development and secure state-of-the-art technology by 2007 occupying 5% of the world RFID / USN market. A later, realisation stage follows in 2010. This aims to occupy 7% ($53.7 million) of the world RFID / USN market, having by then applications to traffic, medicine, environment and logistics.

A promoting organisational structure has been formed, incorporating research institutes and various forum groups. It is planning pilot applications and main projects. These include the following.

- A U-City project, the Songdo special economic zone.
- Public ubiquitous sensor networks.
- A hardware and software architecture and platform for the above.
- The Haroobang pilot platform supporting disaster management and U-Tourism (tested on Halla Mountain and in Cheju University, on Jeju Island).

7 Applications perspective

7.1 Overview

The potential uses of the technology of the Internet of Things are without limit. The conference covered many applications ideas, including:

- current applications earning revenue with a strong business case

- trial and demonstrator applications
- planned applications
- hypothetical applications

RFID applications have established themselves and are here to stay. Technical standards are beginning to emerge. The majority of currently successful applications employ RFIDs in the process of industrial and commercial asset tracking and management. Some of these are "quick wins". One of the presentations claimed that returns on investment within 6-12 months have been achieved. The biggest returns are to be had when tracking is applied to high value, mobile items that hitherto did not have structured handling. The return is likely to be less dramatic in situations where RFIDs replace structured handling using earlier technology, for example barcodes or manual paper-based systems.

The Internet of Things represents a **fusion of the physical and digital worlds**. It creates a map of the real world within the virtual world. The computer's view of the physical world may, depending on the characteristics of sensor network, possess a high temporal and spatial resolution. In other words, it may hold lots of detailed information. The computer's view of the real world need not reflect a human view of the real world, but can free itself of constraints imposed by the limitations of human understanding.

The Internet of Things may react autonomously to the real world. This is known as **proactive computing**[3]. A computer's view of the world allows it to interact with the physical world and influence it. It may run processes that trigger actions, without needing a human to "press the button". Reflecting the requirement for autonomous adaptivity, the following quote was made: "In order to operate at the speed of business, manufacturers have to move from a 'react to forecast' mindset to an adaptive mindset." The Internet of Things is not merely a tool to extend the human capability. It becomes part of the environment in which humans live and work, and in doing that it creates an economically, socially and personally better environment. In industry and commerce, the Internet of Things may bring a change of business processes.

The redesign of business process is not necessarily straightforward. Some applications may function without human input. In other cases, human attendance and involvement will be difficult to remove, even at the simplest level of having someone to push the button and say, "Go." Some applications may aim at supplementing, aiding and enriching rather than replacing the human control of a process.

The automotive sector is likely to be a major user of the Internet of Things. It was stated that the proportion of cars containing inbuilt telematics would rise from 20% in 2007 to 43% in 2010. The motivations for using on-board radio, notwithstanding that this is an electrically difficult environment for wireless transmission, were configurability, flexibility, innovation and simplification of manufacture. An in-car telematic platform and architecture were under development. This sector would use communications for:

- in-car monitoring
- in-car telematics

[3] Terminology introduced by Intel

- car-to-infrastructure and infrastructure-to-car communication
- vehicle-to-vehicle co-operation

Manufacturers may use sensor technology to create extended products. This adds value to physical goods by providing a service element. Robot technology is today normally associated with manufacturing and business; however one presentation suggested that the home robotic market might exceed the industrial market within ten to twenty years' time. The home market, notably the healthcare sector, adds extra requirements for lightweight, wearable devices.

The development of successful applications depends on the development of technical platforms and where appropriate standards within the application domain. These include:

- Service object architecture (SOA)
- Digital manufacturing
- Flexible manufacturing
- Manufacturing intelligence
- Data mining
- Data management
- Manufacturing and user interfaces
- Usability
- Product representations
- Means of personalisation

Sensor networks and pervasive networking approaches are also of high interest to the mobile industry. Context aware applications using mobile devices with dynamically varying service platforms are currently under investigation by mobile operators. Pilots already exist showing the possibility of using a mobile device to interact with the environments, e.g. in various consumer contexts. A major EU manufacturer has also launched an initiative called "Sensor Planet", which consists of a test platform for mobile-centric wireless sensor network research. The vast majority of the research challenge in the context of mobile communications with devices is related to the service platform and to the requirement of making available "context aware services" that can dynamically react and adapt to the environment.

7.2 Application list

There now follows a list of applications raised at the conference, organised into a simple logical taxonomy. This report does not claim to have captured every possibility that was either stated or implied in the presentations and discussions. However, it gives a view of the spectrum of possibilities. Many more may be imagined. Note that there are no obvious "killer" applications. This is an added reason why a standard infrastructure is necessary, as opposed to leaving it to the market to create application-specific infrastructures in a piecemeal fashion. This in turn drives the requirements towards development of generic technologies that may be subsequently reused in diverse application contexts.

Military applications

Oil & gas industry

Mining industry

Intelligent buildings

- Building automation

Transportation

- Monitoring railway vehicle bearing temperatures
- Predictive mid-life maintenance
- Monitoring early-life performance
- Transport logistics
- Shipping
- Ticketing and payment
- Mobile phone interacting with payment systems

Automotive

- Intelligent tyre
- Vehicle identity
- Motorway signs
- Vehicle to vehicle, co-operative driving
- Internal vehicle control architecture
- In-vehicle telematics
- Infrastructure-to-vehicle communication: road and service information
- Recycling of materials in vehicles
- Detection: seat belts, door / trunk opening, temperature, rain
- Parking sensing

Environmental monitoring

- Tagging bird population
- Meteorological monitoring
- Radiation detection
- Coastal and wave monitoring
- Tsunami detection
- River level monitoring
- Water pollution monitoring
- Golf course ground management

General supply chain and product management

- Supply chain integration
- Product life cycle integration
- Inventory management
- Spare-part warehousing
- Warehouse management
- Warehouse batching for delivery
- Quality control
- Serial number look-up
- Field service management

Mobile asset management

- Airport secure vehicle tracking
- Aeroplane maintenance tools tracking
- Pallet tracking
- Scrap handling
- Hazardous waste management
- Geolocation

Process management

- Semiconductor wafer fabrication, batch movements
- Industrial robotics
- Telerobotics (distant robot control)
- Telepresence: camera / video recorder
- Gas pipeline monitoring

Compliance monitoring activities

- Fire shutters
- Fire doors
- Smoke alarms
- Escape routes
- Premises cleaning
- Conveyor systems

Agriculture

- Monitoring of food supply chain (“from field to fork”)
- Monitoring of animals
- Plant protection

Retail management

- Shelf stocking
- Shopping basket / shopping list
- In-store direction finding
- Display advertising
- Sensor-based checkout
- Vending machines
- Tagged merchandise
- Mobile phone interacting with payment systems
- Hired equipment tracking

Healthcare

- Drug identification and tracking
- Healthcare monitoring: ECG, pulse, temperature, blood pressure
- Life support monitoring

Security

- Detection of counterfeit goods
- Access control
- Banknotes
- Passports

Government and public sector

- Disaster management
- Tunnel fire management
- Tourism support
- Homeland security: special event control

Information systems

- Billboards and signs

Home

- Remote door lock monitoring
- Remote home metering
- Follow-me visual communication
- Home appliance network
- Home automation
- Home robotics

- Lifestyle assistant (follows you, helps you find things)
- Lifestyle: lighting control
- Lifestyle: choosing music, TV programmes
- Entertainment environments
- Food monitoring ("internet fridge")
- Energy management
- Automatic shutters

Leisure and recreation

- Sports equipment: user performance monitoring

Education and learning

- Intelligent teddy-bears (talk, demonstrate scientific principles)

8 Non-research perspectives

This section of the report addresses non-technical issues of possible concern to governments, regulators and other policy-making bodies. It captures the proceedings of the final session of four presentations and the preceding panel discussion.

8.1 Closing session

The important issue of **naming and addressing** was outlined. If one wants to connect with something, one must know where it is. In the Internet, a hierarchy of **domain name servers** (DNS) allows one to do this. The root server is queried, which directs to another server, and so on, until the one that knows the physical address is found. An extension of this system, **object name servers** (ONS), is expected to serve RFIDs and the Internet of Things. There is a governance issue because name servers are owned resources that confer monopoly control of data on their owners. Problems have already surfaced within the Internet's existing DNS system. The Internet of Things presents a further challenge that mobile objects may need to re-register their presence on different name servers as a consequence of moving. This requires redelegation, redelegation requires authorisation and authorisation needs means of controlling the authority, or else someone could steal the identity. The Internet of Things must learn from the DNS discussions. The presentation further crystallised the problem thus: "(Though) the end node is no longer under control of the network provider, and neither are the services, network providers might use RFID as yet another application they want to control, instead of seeing it as another end-to-end solution using their network."

The second speaker listed many issues, including access, roaming, billing, legal liability, data retention, competition, privacy and threat vulnerabilities. This was a timely distillation of issues generic to many types of network, as any of these could in due course become a hot button issue.

The privacy position was also reviewed, noting that RFID technologies provide for identification of people and collect data about their personal activities. Applications may be:

- mandatory (e.g. passports, identity cards)

- conditional but without a realistic opt-out (e.g. transport payment)
- conditional with opt-out facilities (e.g. tag neutralisation, loyalty card contracts)
- genuinely optional (e.g. personal enhancement, sports applications)

It was concluded, "RFID smart tags are not, by themselves, a threat against privacy (or business secrets), but unsecured, non-publicly regulated information systems supporting RFID-empowered applications definitely are." Hence, a need for additional privacy regulated regulation was called for.

Reviewing the present state of the European legal framework in protecting sensitive personal data, it was also noted that since the directive entered into force in October 1998, the Commission has not received notifications from the UK, France, Italy, Ireland, Sweden or Luxembourg. Furthermore, none of the new ten Member States has yet notified the use of contractual clauses or other safeguards to the Commission.

Radio is fundamental to the Internet of Things, and the allocation of **radio spectrum** is possibly the most important key issue for many regulatory and government agencies. A number of proposals were put forward.

There are four ways to allocate spectrum to users and applications:

- managed methods, the traditional "command and control" model
- market methods, the "property" model
- unlicensed spectrum methods, the "commons" model
- mixed methods, using a combination of the above methods according to function and economic purpose

Although we are unsure which of the methods will catalyse maximum economic growth, recent studies are pointing in the direction of the last two.

Growing demand for radio usage implies either the spread of unlicensed bands in breadth and number, or the spread of new technology which:

- allows transparent overlap of multiple signals (direct spread spectrum)
- adapts and compensates for already occupied spectrum with cognitive radio and software defined radio

Against the belief that spectrum is scarce, it was argued, "Today's spectrum scarcity is very much an artificial product of archaic public policies." Quoting Mark McHenry, the speaker went on to say, "On average, only slightly more than 5% of the USA radio spectrum is used nationally at any given time." Hence, the need for revisiting the way spectrum is managed was outlined, which is an issue not constrained to the RFID applications, but ranging across all applications of radio spectrum.

8.2 Panel discussion

The discussion explored a number of issues.

- The most important research topics
- Funding priorities
- Why is public funding necessary?

- How can research be accelerated?
- What about privacy and the ethical dimension?
- Should we qualify software for quality and security?
- Will the automotive industry trust an external sensor?

The most important research topics, according to panel members, would be system dependability and system integration. The need to take a system perspective encompassing all the various issues was reaffirmed.

Funding priorities should support a long-term perspective. Fundamental, "blue sky" research is going to be essential, though it needs to be strongly articulated with industrial perspectives.

Companies must share the true problem issues with the academic world, not letting confidentiality concerns obstruct this.

How can research be accelerated?

The simple answer is that it probably cannot. Truly creative innovation needs time. We can, of course, try to stop the spending of research time on less creative paper chase activities. Infrastructure issues are in general related to long innovation cycles, because of the magnitude of the required investments.

What about privacy and the ethical dimension?

This question provokes two types of response. The first is that privacy should be a primary and urgent concern, even to the point of slowing development of the technology. The second is to say, "Forget it. Pandora's box has opened and cannot be closed, privacy is lost, the technology is interesting, so let's get on with it."

This last view must, in its extreme form, surely be unacceptable. A presentation reminded, "One of the most fundamental rights in a healthy society is the right of every citizen to be left alone. Article 12 of the UN Universal Declaration of Human Rights, states that 'No one shall be subjected to arbitrary interference with his/her privacy, family, home or correspondence.' "

It follows that governments must give emphasis to a legal framework that will cause these issues to receive right consideration.

Should we qualify software for quality and security?

This is a good objective, but the panel doubted that throwing tools at checking for quality would be productive.

Will the automotive industry trust an external sensor?

It is most unlikely that in-car systems will trust life-critical decisions to external systems in the short term.

9 Annex: conference agenda

9.1 Welcome address

Dr João Da Silva, Director Network and Communication technologies,
European Commission, DG Information Society and Media

9.2 Stream A1: State of the art & vision – the system and technological perspective

This stream aimed to provide vision on future evolutions towards pervasive networked systems and devices, with a mid-term to long-term perspective. It was intended to give insight into the various economic, technological and application trends driving the evolution of the architectures to be considered for future systems of "networked objects". The stream aimed finally to introduce open technological issues and generic future challenges at system level.

Session Chair: Prof. Ramjee Prasad, University of Aalborg

Research Views
"Wireless sensor networks: is it worthwhile after at all?"
Prof. Petri Mahönen, University of Aachen
"Ubiquitous digitisation: connecting people and objects to people and objects"
Dr. Pekka Silvennoinen, Director, VTT Technical Research Centre of Finland

Industry Views
"From smart devices to ambient communication"
Dr. Gilles Privat, Senior Scientist, France Telecom R&D Division
"The Internet of Things"
Dr. George Bilchev, Pervasive ICT Centre, BT

A view from the ITU
"Pervasive, ambient, ubiquitous: the magic of radio"
Mrs. Lara Srivastava, New Initiatives Programme Manager, ITU

Concluding remarks, bridging research and business
"Bridging the gap between research and business in the on demand era"
Dr. Krishna Nathan, VP Services, Director Zurich Research Laboratory, IBM

9.3 Stream A2: The security, privacy and society dimensions

This stream took a system perspective of the various security issues that can be encountered in pervasive networked systems having to support high flexibility and reconfigurability constraints.
"RFID-Tags: Privacy and Security Issues"

Dr. Pim Tuyls, Senior Scientist, Philips Research

"How to secure visible, physical, (of only one holding) objects through a digital trustworthy infrastructure?"

Prof. Michel Riguidel, Head of ICT Dept, Ecole Nationale Supérieure des Télécommunications (ENST)

"From central command & control to distributed dependability & empowerment"

Dr. Stephan J. Engberg, Founder, Open Business Innovation, Priway

"Privacy, ethics and society: implications of pervasive computing"

Dr. Frank Stajano, Lecturer, University of Cambridge Computer Laboratory

"RFID in asset management: European case studies"

Mr. Paul Stam de Jonge, Group Director - RFID Solutions, Logica CMG

9.4 Stream B1: The application and industrial perspective

This stream aimed at a mid-term to long-term perspective in identifying requirements for future applications taking advantage of pervasive networked technologies such as RFID and their likely evolution towards smart objects.

Afternoon Session Chair: Prof. Michel Riguidel, Head of ICT Dept, Ecole Nationale Supérieure des Télécommunications (ENST)

"The Internet of Things in production, logistics, and services"

Prof. Dr. Elgar Fleisch, Institute of Technology Management, University of St Gallen
"Pervasive networked technologies for automotive application"

Ing. Francesco Lilli, Head of Technologies Department, Telematics Systems, Centro Ricerche, FIAT

"The Internet of Things: - an industrial perspective"

Dr. Martin Elixmann, Head of the Connectivity Dept, Philips Research Europe (Aachen)

"Proactive computing: RFID & sensor networks"

Mary Murphy-Hoye, Senior Principal Engineer & Joe Butler, Co-Director, IT Research, Intel Corporation

9.5 Stream B2: The application and industrial perspective (continued)

"Intelligent and networked products: a product and manufacturing perspective"

Prof. Dr.-Ing. Klaus-Dieter Thoben, University of Bremen

"RFID activities at Siemens: from shop floor to board room"

Dr. Claus Biermann, Corporate Technology, Siemens

"Ubiquitous sensing, computing and communication"

Dr. Tapani Ryhänen, Head of Strategic Research, Mobile Devices, Nokia Research Centre

"An application and industrial perspective"

Prof. Dr.-Ing. Hendrik Berndt, CTO, DoCoMo Euro Labs, Munich

9.6 Stream C: Snapshot of IST initiatives

This stream introduced the main research topics of a number of running or completed IST projects in the field of pervasive networked devices, outlining the main challenges for future collaborative R&D.

Morning Session Chair: Mr Rainer Zimmermann, European Commission

PROMISE (enterprise management): "Smart Items & Future Manufacturing"

Dr. Uwe Kubach, Director, SAP Research, Dresden

EYES (objects networking) project overview

Dr. Nirvana Meratnia, Researcher, University of Twente

e-SENSE (RFID/objects networking): "Capturing ambient intelligence for mobile communications through wireless sensor networks"

Dr. Pierre R. Chevillat, Manager Sensor Networks, Zurich Research Laboratory, IBM

MAGNET (PAN/BAN): "The unpredictable future: personal networks paving the way towards 4G"

Mr. Juha Saarnio, Head of Industrial Initiatives, Nokia

An overview of the RUNES project

Dr. Cecilia Mascolo, Advanced Research Fellow and Senior Lecturer, University College, London

UbiSec&Sens (security aspects of networked objects) overview

Dr. Dirk Westhoff, Senior Researcher, NEC Labs Europe

CRUISE (Network of excellence on technologies)

Dr. Ir. Neeli R. Prasad, Head of Wireless Security and Sensor Networks Lab, Aalborg University

9.7 Stream D: Beyond Europe

This stream presented views from the US and in Asia on current and expected developments in the field of networked ubiquitous systems and smart networked devices.

The USA: Prof. Dr. Ian F. Akyildiz, Georgia Institute of Technology

Japan: Dr. Shingo Ohmori, Vice President, National Institute of Information and Communications Technology (NICT)

Korea: Prof. Dr. Daeyoung Kim, Auto-ID Labs Korea Information and Communications University.

9.8 Panel Discussion: evolution & collaborative research requirements

Afternoon Panel Moderator and Session Chair: Prof. Petri Mahönen, University of Aachen

The moderated panel discussion gathered speakers from the morning presentations and other contributors, providing an opportunity for exchange of views and interactive debate with the audience.

Previous speakers included Ian Akyildiz, Pierre Chevillat, Cecilia Mascolo, Neeli Prasad, Ramjee Prasad, Frank Stajano and Dirk Westhoff. Others, not being previous speakers, were Prof. Gianfranco Manes (University of Florence) and Dr.-Ing. Andreas Willig (Technical University of Berlin). There were questions and contributions from the audience.

9.9 Stream E: Possible barriers to deployment

This stream went beyond R&D issues to address economic, privacy, regulatory, policy and consumer acceptance issues that follow from the implementation of networked pervasive technologies.

"A brief look at ONS and DNS, and Internet of Things"

Dr. Patrik Fältström, Member of Internet Architecture Board, Senior Consulting Engineer, Cisco

"RFID tags & ambient, ubiquitous networks" (Consumer and privacy issues of ubiquitous technologies)

Dr. Ewan Sutherland, Former Executive Director, International Telecommunications Users Group (INTUG)

"From digital object identification to digital identification of people: institutional answers tested by reality"

Dr. Françoise Roure, President, Legal and Economic Section, National Advisory Board on Information Technologies

"The issue of spectrum: radio spectrum management and ubiquitous network society"

Mr. Simon Forge, SCF Associates Ltd

****