

Answer to the European Commission public consultation on the early challenges regarding the "Internet of Things"

Please indicate your preference (use a X):

- I agree that this document is made public
 I want this document **not to** be made public

If you reply on your own behalf, please indicate:

- Name:
- Telephone:
- Email:
- Country of residence:

If you are replying on behalf of an organisation, please indicate:

- The organisation's name: Eurosmart
- The type of organisation:
 - private company
 - government/public body/international organisation
 - academic/research institution
 - non-governmental organisation
 - other: non-profit association
- Your organisation details
 - o location: Rue du Luxembourg 19-21, B-1000 Brussels
 - o size: 25 members
 - o scope of activities (max 3 sentences):
Founded in 1995, Eurosmart gathers 25 companies representing the whole value chain of the Smart Security Industry. The Association is committed to expanding the world's Smart Secure Devices market, developing smart security standards and continuously improving quality and security applications. Eurosmart is the ideal forum to value the expertise of the Smart Security Industry regarding security, and privacy management in particular.
 - o website: www.eurosmart.com
- Contact person: Sabrina POCHERON
- Contact person' telephone: +32 2 506 88 38
- Contact person's email: sabrina.pocheron@eurosmart.com

Please start replying on the next page

The Commission Staff Working Document describing the challenges and technologies that will enable the Internet of Things is a very comprehensive, very accurate vision that Eurosmart has been sharing since its early birth. Eurosmart Members are convinced that with the completion of a ubiquitous, global and mobile Internet, many stakeholders will have a vested interest to built connectivity into their products to bring new services, more productivity, more efficiency. For the same reasons people can trade very valuable information, “objects” will also trade pertinent data to improve everything from their life cycle to the way they get used, sold, stored or disposed. The Internet of Things as defined in the vision of the European Commission goes far beyond a smart wireless logistics management tool. It is more like a network of objects collaborating with each other and with humans to bring more value, more services, and more knowledge.

As an Association gathering 25 companies representing 65% of the Smart Security Industry and embracing the entire Embedded Security Industry (Silicon, Software and Smart Secure Devices manufacturers), Eurosmart is a privileged actor of the deep changes that are taking place in the digital world. The smart card industry has developed over the years a know-how about Security, Privacy and over-the-air life cycle management of Smart Secure Devices that will support and enable the Internet of Things revolution. Thanks to RFID and biometrics technologies, smart cards shapes are quickly changing into what we call Smart Secure Devices. Thanks to nanotechnologies, those Smart Secure Devices will be made cost effective and small enough to fit into billions of objects that will be connected to the Internet. Beyond communication, Smart Secure Devices applied for the Internet of Things will protect the data and manage access rights and credentials, just like smart cards do today for people.

Smart and Secure RFID and NFC

For Eurosmart, the Commission Staff Working Document should establish a clearer distinction between secure contactless objects and RFID circuits.

If contactless products, based on RFID technologies, are today deployed all over the world in various applications like good traceability, transportation ticketing, financial transactions, access control, identity cards, or e-Passports, all these applications offer totally different levels of security and privacy to the user.

In the case of RFID Tags used for identifying an object or an animal, there is little to no protection needed, minimal data storage, low cost and some time long distance reading. Some basic security functions such as passwords and hard-wired crypto features can however be integrated in RFID Tags at low cost.

In the case of a Secure Contactless Device in an e-Passport, there is a maximum protection needed with amount of confidential protected data stored, encrypted communication and short distance of transaction.

Against this background, Eurosmart would rather recommend using the term Secure Contactless Device rather than the RFID term as the latter is often synonym of unsecure products.

Considering Micro Electro Mechanical Systems

Micro Electro Mechanical Systems technologies should be considered when dealing with emerging “enabling technologies”. MEMS will be indeed a key enabler of the Internet of Things deployment. By enabling nano-scale, low cost and event-powered sensors embedded into objects, pertinent alarms or context-based messages will be traded by objects via the RFID bearer and the IPv6.

There are two types of information that objects can carry with them (and trade with other objects or with humans).

- Resilient information: Data that are stored and permanent, such as a brand name, a product name and other detailed information such as a built date, a built place, an expiration date, operating conditions, etc... Resilient data aim at being used by humans or machines that will have to deal with the “object” during its life cycle. Amazingly, technologies to render resilient data today are extremely basic (text notice, bar code, etc...) and RFID alone brings a little revolution in that area by enabling contactless, at-a-distance acquisition of such data. RFID being an integrated circuit potentially personalized for each object, the amount of resilient data that each object can carry is also multiplied by thousands or millions compared to old, primitive technologies.
- Dynamic information: With the help of sensors (temperature, pressure, pH, light, current, horizontality/verticality and many more) combined with heuristics, stored as resilient data, and defining ranges of operations to setup alarms or warning messages, now objects can acquire information from their environment that is pertinent to them, and to other objects and people operating with them. That is the potential that MEMs offer for the deployment of the Internet of Things.

Security and Privacy

If the vision of a network of objects trading information and the benefits are clear, security and privacy between people are needed for the same reasons. Eurosmart fully supports the position of the European Commission concerning the necessity to define what/when/with whom objects can communicate and particularly welcomes the Recommendation on the implementation of the privacy, data protection and information security principles in applications supported by RFID, as well as the Communication on Privacy and Trust that the European Commission intends to present.

Solutions for a secure and safe Internet of Things guaranteeing the protection of individual data and the respect of privacy are already available. Eurosmart Members are already delivering Smart Secure Devices (SSDs). Eurosmart defines a Smart Secure Device as *“a Smart object which contains a Secure IC and embedded software and supports personalization by the issuer; the main purpose is to offer Human to Machine as well as Machine to Machine security services such as data integrity, user authentication or secure storage. It comes in multiple form factors, including Smart card and Smart USB Token. It includes personal, portable as well as embedded devices”*.

Examples of SSDs are Smart USB Token which represent microprocessor-based, personalized devices to enable secure transactions on behalf of a Service Issuer for its

end-users, or communicating Smart M2M modules. M2M initial vision is a use of Telecom Networks to allow machines to be connected together. The Smart M2M device is pretty much a 3G modem for data services. In a later step, i.e. the deployment of the Internet of Things, the IP protocol will be used to connect objects within a close vicinity using RFID and our role (SSDs) will be to manage credentials and secure transactions between objects.

Regarding the personalization of SSDs, Eurosmart would like to stress the importance of maintaining/updating the credentials as they do evolve over time. The model where personalization of the Smart Secure Device is done once for good during the production phase is not obsolete, but it needs to be complemented by a secure over-the-air tunnel to maintain/update the credentials. In the case of RFID-connected objects, it implies the emergence of new technologies to support ad-hoc networks since such objects are not intended to be reachable by traditional broadcast or unicast networks. Interestingly, the Internet today already realized that the vast quantity of computers linked by a network builds The Computer. Sharing resources and sharing data is a path to more efficiency and more productivity so the computer world is also discovering the power of mesh-computing. In the Internet of Things strategy, Eurosmart Members will leverage on today's OTA technology based on broadcast or unicast networks to expand it into the ad-hoc model. Point-to-Point security will have to work in a mesh model, with an infinite amount of node points passing the data.

Standards for the deployment of SSDs are already available and can ensure the interoperability between the participating systems. Eurosmart is strongly committed to their development and fully supports the willingness of the European Commission to encourage open, interoperable and publicly accessible European standards. Our Association has been able to provide relevance advice on interoperability requirements and can highlight the advantages and potential of existing middleware technologies for the e-ID EU wide systems.

Final comments

To conclude of these remarks and to re-emphasize the support of Eurosmart Members about the Vision and the challenges that the European Commission identified, we do feel that the lessons learnt with Smart Cards will not only apply to, but also be a condition of success for the Internet of Things. Eurosmart Members know what needs to be done: RFID and MEMS technologies need to reach cost and performance levels to be in line with the value created by the communication between objects. Smart Secure Devices will have to deliver Contact-like security and privacy in the contactless world, over-the-air provisioning to ad-hoc networks will need to be expanded, and Smart Secure Devices will need to be smaller and smaller, beyond what human eyes can see.

Eurosmart members are convinced about the Value that the Internet of Things will bring to all its stakeholders. We are convinced about our industry's ability to built Security, Privacy and Ease-of-use to communicating objects, like we did for Human to Machine transactions. We are also convinced about the fact that the accountable Authorities have a clear vision of their role to enable the eco-system, and will take actions to support its success.