



Future Networks and the Internet Early Challenges Regarding the „Internet of Things“

*Joint comments by AIM-D, BDI, BITKOM, GS1 Germany, HDE,
and Informationsforum RFID*

November 2008

In September 2008 the European Commission presented the staff paper «Future networks and the internet – Early Challenges regarding the „Internet of Things“» and asked for comments regarding the issues covered therein. The staff paper explains the vision of an Internet of Things and describes potential applications. Then, it identifies RFID technology as first step and basis of the Internet of Things and develops policy challenges for the Internet of Things from the point of view of the EU Commission. The staff paper will be the basis for a European Commission Communication, which will be published in 2009.

Informationsforum RFID, the German Association for Information Technology, Telecommunications and New Media (BITKOM), the Federation of German Industries (BDI), the German Retail Federation (HDE), GS1 Germany, and the industry trade association AIM-D welcome the efforts of the European Commission to actively and timely accompany the development of the Internet of Things. Since 2006 the European Commission shaped the political debate about RFID through expert workshops, consultations, setting up of an Expert Group, funding of various projects, and numerous publications. The staff paper as predecessor of a Communication on the Internet of Things shows that the EU Commission continues this work and puts great emphasis on this development.

The staff paper covers all relevant issues of the political debate and puts them into the right context. Most assumptions and conclusions correspond to the facts or the assumed developments. We welcome the fact-based view upon this technology that also leaves sufficient room to develop future scenarios and draw policy conclusions. Chances and challenges are being assessed realistically as far as this is possible.

RFID AND THE INTERNET OF THINGS ARE NOT IDENTICAL

For an exact consideration of the Internet of Things clear definitions are necessary. This is true both for the Internet of Things itself and for connected technologies. Also, further and related notions such as the Internet of Services and web 3.0 should be considered by way of addition or differentiation.

During the development of the Internet at first computers were combined to a network. Thus, these could be reached in the new virtual world. Some time later, companies and single persons followed, who found their place on the Internet via their own homepages and later via blogs and social networks. These virtual placeholders often offer information on availability and state of a person, company or institution. This data is always accessible and can, in combination with e-mails and chats, be used for communication. In parallel, networks of mobile devices developed so that the Internet was available everywhere.

In the Internet of Things, objects will follow onto the Internet. Each object will obtain its own homepage where all relating information is stored and, thus, can be accessed. Whether this data is stored on a server or directly on the product does not matter; the decisive factor is that the data is available via the network. The link between object and data is made possible e.g. through an RFID transponder. So far, simple and cheap substitutes such as 2D codes are used as well; however, automation is very limited in these instances. Origination data is created by the linkage of object and storage medium and is amended automatically by further data at each reading point.

The ensuing unique identity will enable networked objects. However, the network will only become intelligent through the expansion of transponders by way of sensor technology and computing power. The latter will also enable security through cryptography. In addition, energy supply and miniaturization are important prerequisites for a successful implementation. Therefore, a restriction of the Internet of Things to RFID technology falls short of reality and is a weak spot of the document.

ARCHITECTURE

The basics of the architecture of the Internet of Things listed in the document correspond to the current status and are addressed correctly. However, it is difficult to compile a solid prognosis on this basis since an equation of the Internet and the Internet of Things must be avoided despite structural similarities. So far, the Internet of Things is largely only a vision so that specific statements regarding its architecture are not yet possible. In addition, it is unclear whether there is going to be only one single architecture and how it will be used in the future by the different applications. The same is true for the architecture of complex RFID systems. The networks developed so far for RFID applications serve for testing and gathering experiences. There is no network yet that implements all requirements of an open RFID system, much less of the Internet of Things.

Despite the limited significance of today's networks there are assumptions that already today possess a very high probability. For instance, one can assume that the Internet of Things will not simply use or copy the structures of the Internet. Rather, parts of the Internet may become part of the Internet of Things and may be used for data transmission. However, large parts of the data bases and structures will exist in parallel because they will have to fulfil different requirements. For example, different access rights must be enabled and autonomous systems must be integrated. On this basis companies and organizations currently develop and test models. It is too early to predict when a system will be established and what it will look like.

FREQUENCIES

All considerations regarding the Internet of Things must keep in mind the implementation that follows. This is true in particular for network capacities and transmission bandwidths. For RFID, especially UHF, a sufficiently broad frequency spectrum is necessary to enable the large number of event-oriented readings at the RFID antennas. It can be foreseen that the spectrum at the air interface (between transponder and reader) currently available in Europe will not suffice. Without an increase there is a risk of competitive disadvantages compared to other world regions.

Therefore, regulators should already today allocate the area between 915 and 921 MHz for RFID as further spectrum as recommended by ETSI. The corresponding ETSI System Reference Document was finally adopted resp. presented to the ECC committees in June 2008 (cf. ETSI TR 102 649-2). In addition, it must be ensured for the future that there is sufficient spectrum for the further development of the Internet of Things.

SECURITY

The staff paper correctly recognizes and lists the challenges for the security of the Internet of Things. However, in this context as well it is of utmost importance to clearly distinguish the Internet from the Internet of Things. As regards security in particular, the architecture of the Internet of Things can be expected to be significantly more restrictive than the architecture of the Internet. For users to be able to rely on the security of the Internet of Things they will most likely keep and administer important segments in their own systems. It can be assumed that attacks known today from the Internet such as spam will not represent a particular hazard as regards the Internet of Things. In addition, the physical connection will allow for new protection functions, e.g. by using the coordinates space and time as protection. Thus, it could be regulated that data can only be exchanged when it is space- and time-related to the order.

At the same time, the new interface to the real world creates new challenges that are so far not mentioned in the staff paper but should be considered. The radio transmission of data makes the data susceptible to interferences and eavesdropping attacks. Tags can be removed, destroyed, or blocked. Not only does the radio transmission require sufficient spectrum, it must also be protected against unlawful eavesdropping and manipulation. This requires new solutions and the creation of technical guidelines. An important first step in this context is the Technical Guideline RFID of the Federal Office for Information Security whose first part was published in November of 2008.¹

In addition, the Internet of Things will provide security as well. The tracking of supply chains and unique identification possibilities create new protection measures against piracy and theft.

APPLICATION AREAS

Based upon five examples the staff paper shows the future opportunities and the potential of the Internet of Things. These examples are sufficiently broad; however, their depth varies considerably. Especially the last example “Environment” is not exhausted by the description. Knowing which object is available where and in which state would make many production, delivery, and information processes much more efficient. Unnecessary routes, empty runs, over-capacities, provisioning, and searches could be significantly reduced. At the same time, the exact tracking of specific steps would enable a better computation of the CO2 footprint of products and services; thus, critical processes could be better analyzed and calculated. On this basis, both companies and consumers could evaluate products and services in a better and more targeted way. In addition, environmental consequences could be more easily examined as to their causes and, thus, addressed.

Another example demonstrating the potential of the Internet of Things is asset management. Already today one can find many RFID applications in this field. However, the further linking and e.g. the using of sensor data will considerably simplify the administration of safety-relevant tools, enhance lifecycle tracking, and, at the same time, improve occupational safety.

Further, the staff paper should additionally address the issue of accessibility. With the support of the technology, blind and visually impaired people could experience their environment using electronic tools. In particular, they could notice traffic signs more easily, recognize and use public transport and timetables, localize and detect objects in apartments without touching them, or find products in stores. Senior citizens could have processes automated even without having to have a specific technical understanding.

¹ <http://www.bsi.bund.de/literat/tr/tr03126/BSI-TR-03126-1.pdf>

Finally, the staff paper does not consider that most likely new networks with similar functions that resemble today's Intranets will establish themselves besides the generally accessible Internet of Things. Partly, there will later merge with the Internet of Things, partly they will co-exist, for example because they have different security requirements or were developed from the beginning for a specific user group. Some companies plan, for instance, to work with cascaded responsibilities and not enter all information into a broad network. However, through interfaces these networks could at least partially become part of the Internet of Things as well. An example more and more often mentioned in this context is the Intranet of Goods, which combines today's vision of RFID solutions and network-based solutions: A transparent supply chain, information regarding storage and sales area, special consumer offerings on the sales floor and after the sale would be the consequences of an Intranet of Goods. Further examples can easily be conceived.

POLITICAL CHALLENGES

The possibilities of the Internet of Things will result in significant changes for business and society. This leads to challenges that should be addressed as early as possible by political decision makers. The staff paper lists six specific challenges of particular relevance. However, these examples focus unilaterally on societal challenges and neglect economic issues.

The development and introduction of innovative technologies is of great significance for Europe. High production costs and demographic change in an increasingly globalized world require particular efforts to maintain competitiveness. In its 2007 Communication "Radio Frequency Identification (RFID) in Europe: steps towards a policy framework" the EU Commission attested RFID great potential in this regard. As the Internet of Things will possess even further-reaching possibilities, politics should focus on these chances in the future as well. The appropriate framework to continue to position Europe well with regard to future technologies must be created today.

Economic success in Europe requires not only large corporations but also small and medium-sized enterprises (SME) to continually increase their competitiveness. In numerous projects both the EU Commission and the Member States make an effort for SME to get to know and utilize innovative technologies such as RFID. However, a current study of Informationsforum RFID in cooperation with the Research Institute for Telecommunications (FTK) shows that while SME have great interest in RFID they significantly lag behind large corporations concerning implementation. As SME are key for the development and introduction of the Internet of Things both as users and as providers of the technology, this result can be taken as a warning. SME often do not have the financial and human resources to inform themselves about new technological opportunities and invest in complex new technologies. Targeted information, funded networks, and support for pilot projects can be ways to involve this group in the development of the Internet of Things.

Further challenges are research and the implementation of research results. Europe has excellent research facilities and is leading the field as regards the Internet of Things. In addition to basic technological research, applied research is an important part of the development of the Internet of Things. Due to the width of the research field the funding of research clusters is of great significance. In this context, the EU Commission's ICT PSP is a positive example that should be expanded and used as example for other programs.

STAKEHOLDER INVOLVEMENT

The staff paper points out correctly that the development of the Internet of Things is a long process. Much remains a vision that still needs to be implemented. Single applications are close to maturity; however, these do not create an Internet of Things. Therefore, a step-by-step approach is necessary that accompanies, promotes, and brings together the develop-

ment. In this context, it is particularly important to involve and link all stakeholders. Determinations that are made too early can slow down or even endanger the entire process. The EU Commission's call for a Thematic Network for RFID in the ICT PSP framework is an excellent basis for collaboration. The cooperation of initiatives, institutions, research, businesses, and policymakers offers an outstanding opportunity for the necessary exchange between stakeholders. When Europe works together on the Internet of Things in an open and future-oriented way, today's vision can be tomorrow's key element for Europe.