

CNIPA (National Centre for ICT in the Public Administrations): RFID actions
Indra Macri
CNIPA

Abstract: CNIPA, supporting the Italian Minister of Reforms and Innovations in the Public Administrations, is promoting the introduction of RFID in the Public Administrations. During the last two years (2005-2006) CNIPA has invited stakeholders - basically Public Administrations, Academic Institutions and the most important ICT Associations - to participate in the working group to define guidelines on RFID in the public sector. The guidelines are addressed to Public Administrations that would like to adopt RFID technology to innovate their processes.

This paper resumes very shortly the results of studies about the economical and healthy impact in the use of RFID.

Introduction

CNIPA (National Centre for ICT in the Public Administrations) has dedicated a working group to RFID, evaluating this technology as one of the factors of major innovation in the processes of Italian Public Administration. The analysis of RFID has been focused also to the problems related to privacy and health, due to the strong impulse from European Commission responsible for Information Society and Media, particularly after the EU RFID conference held at Brussels on 16th October 2006.

Mainly there are four questions that we have asked to ourselves:

1. how RFID works?
2. when and how the adoption of the RFID technology is really convenient?
3. which are the problems about privacy using this technology?
4. which is the effect of RFID on health?

Of course, in this paper we will not report the answer to the first question, because the functioning of RFID is supposed to be well known to the reader.

On the second question has been instituted a specific focus group with the School of Management of "Politecnico di Milano", to study some of the most interesting processes of the Italian Public Administration. We have considered the life cycle of the book in a library, the life cycle of an archaeological find in the Ministry of Cultural Asset and Activities,

for the great importance of archaeology in Italy, the life cycle of a cargo in an Italian harbour, also in the prospective of a connection with the other EU member States. Starting from a deep analysis of these three processes we have understood if and how the adoption of RFID technology would be convenient.

The aspects related to the privacy have been already debated in a regulation of the Italian Data Protection Authority that we do not report for brevity. Although it is not available yet a sort of *user guide* for those who want to introduce the technology in their work, nevertheless the Italian Authority for Privacy has indicated the most important principles that have to be implemented. These indications are published (in English) at the web address <http://www.garanteprivacy.it/garante/doc.js?p?ID=1121107>.

The forth question rises from the huge discussion on medical impact in the use of RFID technology. The analysis, conducted by the University of Tor Vergata in Rome, was born from the strong accent that during the last EU RFID conference the Council consumer has posed on the effect of EM radiation to human body. Cnipa agrees that for a large consent in the adoption of RFID technology is important to have knowledge about the potential consequence of the use of RFID in day life.

With the authoritative contribution of the University of Tor Vergata in Rome, we find out the European and Italian measures related to the EM emission and the range of safety. We also report a specific calculation to give a first idea of the impact of RFID on the human body.

Is the adoption of RFID in the Public Administration convenient? [1]

Of course the answer is: '*it depends*'.

Let us analyse the following three case studies.

The first one is the case study of the Library for Economic Studies of the University of Turin [2]. The model has considered the most important librarian services, in terms of amount of movements: free consultation, assisted consultation (for books in protected area), daily loan, home loan, reference to users, interlibrary services (exchange of books between different libraries). The study has

compared three different models of organization:

- no technology (the actual situation),
- bar code,
- RFID tag.

In the scenario no technology each document is identified from a number written inside and there is no technological support for the operations of loan. The OPAC (On-Line Public Access Catalogue) gives information only on the existence of a copy of that book in the library, but there is no connection with other systems to know if the book is available at that moment. The system of surveillance is based on magnetic band and is not compatible with multimedia stuff (CD and DVD). There is one or more desks for front-office operations, like loan and return.

In the scenario bar code the identification of the book is made with a bar code tag. Optical lectures of bar code, in combination with magnetic band technology, is used to register loans and to manage the inventory. The OPAC gives information also on the availability of the book in the library. The system of surveillance is based on magnetic band. This system is not compatible with multimedia stuff (CD and DVD). There are both self-service desk for loans and also front-office desk for all other operations.

In the scenario RFID the books are identified by a chip based on RFID. The chip is put inside the book or inside the multimedia stuff. On the re-writable chips are written only the information related to the inventory code. Chip works at 13.56 MHz, according to the ISO 15693 standard. For loan and inventory is used RFID technology combined with the magnetic band of the user recognition card. Cheap RFID chip no re-writable are adopted for magazines. For each document there is an EAS (Electronic Article Surveillance) system based on chip RFID. There are self-service desk for loan and return as well as front-office desk for all other operations.

In the library examined about 60.000 books of overall 173.000, 10.000 magazines of overall 32.000 and about 1.000 multimedia stuff will have a RFID tag. The library is open all months, except august, for 276 days per year.

The front-office staff works for 28 hours per day and the model presumes that they will continue to work for the same amount of hours also after the introduction of RFID, dedicating more time to the reference activities. The cost of 1 hour of people that works in front-office/back-office is about 16,5 €/hour.

There are 94.414 visitors per year and 4.150 of them ask for a loan. Many other elements are considered in the model, such as the number of consultation, the number of magazines and books bought per year.

The model has considered for the RFID scenario two units for RFID initialization, lending and return with the assistance of a desk operator, one unit for automatic lending and return, one external box for self return 24h, two gate anti-thefts, one portable terminal RFID, 60.000 tags for the books, 10.000 RFID for magazines, 1.000 tags for multimedia stuff and about 500€ per day for 10 days of installation and training on the job. The estimates are made on the basis of market prices. In the table below is indicated the synthesis of the cost of the different scenarios.

Table I. Case study library: synthesis of costs in no technology, bar code and RFID scenarios.

Library	No technology (€)	Bar-code (€)	RFID(€)	ΔRFID %
investment	-	48.570	87.100	
Annual costs				
back-office	37.125	37.949	34.498	-7%
front-office	58.920	56.026	46.393	-21%
Materials	1.253	1.440	1.871	49%
Inventory	13.313	9.482	4.157	-69%
Reference	57.000	57.000	57.000	0%
Total annual costs	167.610	161.896	143.918	-14%

Δ%RFID represents the percentage difference between the costs with no technology scenario and RFID solution.

The major benefit, in percentage, is connected with the inventory activity, which is the one where there is much movement.

Table II. Case study library: time of pay back and Net Present Value (NPV) in bar code technology and RFID

Library	Time of pay back [years]	NPV [€]
Bar-code	8,50	-26.342
RFID	3,68	5.054

To sum up the investment in the bar-code technology for the case study analyzed is not convenient, while the introduction of RFID is

profitable due to the pay-back time is less of 5 years and the NPV (calculated with a CAGR Compound Annual Grow Rate of 9% in 5 years) is positive.

The more movements are involved in the process the more appreciable are the benefits in the introduction of an automatic identification technology like RfId. For this reason the inventory process is the one that in percentage obtains more benefits from the use of RfId technology.

The second case study has considered the archaeological archive of the "Santuario di Ercole Vincitore", in Tivoli, close to Rome, that is part of the Ministry of Cultural Asset and Activities [3]. This archive stores the finds of archaeological excavating nearby. The model has compared the use of technology with the actual situation, where for each find there is a paper tag. The tag contains the inventory number and a short description. After the classification each find of small dimension is located in a plastic box, following a stratigraphic order. All the information about finds is stored in MS Access database and MS Excel files. The annual operation of inventory is made with a notebook.

Actually the "Santuario di Ercole Vincitore" has 21.484 finds stored. 21.473 of these finds are located in 896 boxes, while the last 11 finds are so large that cannot be put in a box. Each year there are about 250 new finds classified and stored in the box. 15 visitors per years, generally researchers, go to the "Santuario di Ercole Vincitore". The Santuario is open 300 days per year. There are 7 people that work there. The inventory activity costs 16 hours/person. Each hour/person costs about 11,50 €. Up to now there has not been any theft.

The model has considered two different scenarios, one with tags put only on boxes and another with tags put on both, boxes and finds. For shortness we report here a comparison between the actual situation and the second scenario with tags for boxes and finds. The tags work at 13,56Mhz and are ISO 15693 compatible. The identification number of the find is written on the tag. Each person has an identification card for the access in the Santuario. The software sends an error if someone/something pass the gate without authorization. A palm terminal support people in the inventory activity. In this scenario it has supposed to use one palm-terminal able to read/write RfId, two access gate (because

there are two buildings to store the finds), 1 desk for initialization, 1 RfId unit, a software for the management, 22.000 tags for the finds and 1.000 for the boxes, 15 smart cards for users that comes to the archive.

Table III. Case study archaeological finds: synthesis of costs in no technology and RfId scenarios.

Archaeological find	As is (€)	RfId(€)	ΔRfId %
investment		37.754	
Annual costs			
Costs of material	-	55,00	
cataloguing		31,60	
preservation find	21,00	2,00	-90%
Take a find from the archive	9,00	1,00	-89%
Report a find to the archive	9,00	1,00	-89%
Inventory	3.880,00	527,00	-86%
Total annual costs	3.919,00	618,00	-84%

Table IV. Case study archaeological finds: time of pay back and Net Present Value (NPV) in RfId technology.

Archaeological find	Time of pay back [years]	NPV [€]
RfId	More that 35 years	-22.783

To sum up in the specific case considered the introduction of RfId is not worthwhile.

The question is: could different archaeological archive be interested in the introduction of RfId? For the answer it has been conducted a sensitive analysis, changing some parameters, that can mainly influence the benefits of RfId, such as more movements of stuff or less expensive technology.

Nevertheless increasing the number of finds and their movements, and hypothesizing a reduction of the costs of RfId technology of 40%, the value of NPV still remains negative.

In conclusion the investment for the introduction of RfId is not justified in this case study.

The case study of Italian Custom analyzes the use of RfId for tracking goods and cargo [4]. The model has considered two scenarios: an electronic seal put as soon as a container reach an Italian harbour (scenario 1), an electronic seal, read from the loading dock,

that had been attached on the cargo at the beginning of transportation (scenario 2). The analysis has evaluated the convenience of the use of RFID looking up the point of view of both Italian Custom and the dock authority.

The controls on cargo are very important for each Country, to preserve the national security of the consumers that buy goods that circulate in the national market.

In Italy the amount of containers is increasing due to the global market, fed by the emerging economics like India and China.

The model has been developed starting from the Venetian harbour data. The Venetian seaport is a multi-purpose harbour, because it treats all kind of issue: from fuel to all other commercial stuff.

Actually for each container that reaches the harbour there is a mechanical seal with an identification number not re-usable. This seal is not always affordable, because it is possible to tampering it, without understanding if and when it has been altered. The planning office of the seaport authority of Venice sends to the operators the list of movements of containers through a wireless network. All the information about import-export of containers are sent also to the customs offices. Even if the connection between dock authority and custom office is not available everywhere, nevertheless it has been assumed as a presumption in the analysis of both scenarios. Actually Italian custom uses different systems to automatically control the merchandise incoming.

When a container arrives, the dock authority makes a visual check of the integrity and of the identification number of the container and of the seal, comparing them with a paper list or editing a query on a portable system. When the merchandise passes the gate, the finance guard, another Italian authority, controls and registers the information that had been previously sent to custom by automatic application.

In the scenario 2 on each container that gets off the cargo ship there is an electronic seal within the classical mechanical one. The scenario has been evaluated supposing that each harbour adopts an international standard for reading the RFID seal. The antennas positioned in the dock facilitate the recognition of cargos, that can be controlled in their movements. The information about position of container are sent to the custom information system. The electronic seal registers on the chip memory the attempts of

forgery. The electronic components of seal "wake up" cyclically and control the status of integrity of the seal. If there has been a trial of violation the memory of seal can register the date and hour of the usurpation. On the seal can be written the number of container, the date of arrivals, the number of seal. The market offers also seals with sensors able to detect the internal temperature of cargo, the level of radiation, the integrity of container, evaluating the conditions of goods. The electronic seal considered in the model works at the frequency of 433MHz and the power is set so that the radius of action varies from 3 to 6 meters. The RFID readers are positioned on the gates of the harbour and of the areas where are stocked the merchandise. The seals are written and read with a palm device by custom's officers. The information system of customs remains the same, except for the integration with the new technology system that manage information coming from RFID seal. In this scenario the check of the identification number of container is automatic. It can be made by the custom's officer reading via palm device or directly reading the id number by the antennas. The integrity of the container, instead, is evaluated by physical inspection. The controls on number and integrity of the seal are completely automatic. If there is an attempt to open the container can be generated a new number or a led can signal the trial of violation. The palm device reads the seal's identification number and verifies if it is correct. If not, it is able to inform immediately that there is something wrong. The number of containers and their positions are recognized from the antennas based on gates. In this way the custom officer has a complete map of all containers in the dock. The operation of "disembark seen", made by the custom as soon as a container reaches the loading dock, is made automatically, reading the electronic seal.

In the model of Venice harbour the annual mean of containers disembarked is about 70.000, coming from 470 ships. The terminal is open 254 days per year and every day there are about 278 containers in transit. The mean time of permanence of each cargo in the dock depository is about 7 days. The scenario in exam assumes that electronic seals are put on cargo at the beginning of the trip. So the initial costs are due to the cabling of the harbour. On average in the stock there are 1.930 containers contemporaneously. The

cost of the custom officer or finance guard is about 20€ per hour.

Table V. Case study track of containers: synthesis of costs for Italian custom in no technology and RFID scenario.

Custom	As is (€)	RFid(€)	ΔRFid %
investment	-	41.595	
Annual costs			
Activities at the terminal	38.904,00	30.344,00	-22%
Activities at the gates	77.849,00	4.192,00	-95%
Total annual costs	116.753,00	34.536,00	-70%

Table VI. Case study track of containers: time of pay back and Net Present Value (NPV) for Italian custom.

Italian custom	Time of pay back [years]	NPV [€]
RFid	1	174.167

On the point of view of harbour terminal has been considered the costs of stocking the containers in import in the Venice depository. Introducing the RFID is very convenient also for Venice dock terminal, as it is shown by the table below.

Table VII. Case study track of containers: time of pay back and Net Present Value (NPV) for Venice dock terminal.

Dock terminal	Time of pay back [years]	NPV [€]
RFid	1	107.269

This case study has demonstrated that the RFID technology improve on the processes of customs and other harbour authorities when the containers have their own electronic seal and there is a complete traceability chain. In addition there are some inducted advantages in the adopting RFID technology, such as time saving for all import/export custom operations.

How 'healthy' is RFID?

Evaluating an EAS/RFid system (Electronic Article Surveillance based on Radio Frequency Identification) on the point of view of health means to understand the minimum distance of security between a device and a

person that uses the devices or is under a continuous exposition.

In most RFID applications, passive or semi-passive tags are commonly used and they communicate with the reader by energy backscattering. The EM exposure issues are therefore related to the reader units only.

The laws and European recommendations for electro-magnetic fields are:

- ¹ "Guidelines for limiting exposure in time-varying electric, magnetic, and electromagnetic fields up to 300 GHz", (Health Physics, Volume 24, Number 4, April 1998, p.494). This document introduces the limitations of exposure for generic person at work. The maximum values are related to the biological effects on human body.
- ² "European Council Recommendation 1999/519/EC of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz", Official Journal, L199, 30.7.1999., p.59). This document describes the limitation of exposure for inhabitants.
- EN 50357 (also Norma CEI EN 50357) "Evaluation of human exposure to electromagnetic fields (EMFs) from devices used in electronic article surveillance (AS), radio frequency identification (RFID) and similar applications". Contains the procedures of simulation and measures to value EM fields exposure level.
- Standard EN 50364 (also Norma CEI EN 50364) "Limitation of human exposure to electromagnetic fields from devices operating in the frequency range 0 to 10GHz, used in Electronic Article Surveillance (EAS), Radio Frequency Identification (RFID) and similar applications.

¹ : International Commission on Non-Ionising Radiation Protection, <http://www.icnirp.de/documents/emfgdl.pdf>

²: http://ec.europa.eu/enterprise/electr_equipment/lv/rec519.pdf

For the evaluation of the EM fields exposure, two thresholds are conventionally considered: *Basic Restrictions*, related to biological effects, and *Derived Reference Levels*, calculated indirectly and referred to easily measurable physical quantities.

At low frequencies (less than 10MHz) the physical data to monitor is the induced current density into tissues, while at higher frequencies (more than 100kHz) the measurement of the Specific Absorption Rate (SAR) is required. The SAR is defined as the power density absorbed by human body for mass unit. Induced current and SAR depend on both the intensity of EM field and on the position of device respect of human body. The thresholds for occupational exposure (adults consciously exposed to EM radiation) and general public exposure with people of all age are different. Limitations for general public exposure are more strict, because common persons are not aware of the danger.

The Derived Reference Levels are not directly connected to a biological effects. They are deduced or measured in absence of the human body. The reference levels are calculated from basic restrictions, supposing maximum coupling between EM field and individual. Also in this case the thresholds are different for occupational exposure and general public exposure. If there are simultaneous exposure to more frequencies the effects must be properly added (guide lines ICNIRP).

Italy has established in the law n. 36 of 22/02/2001 ("Protezione dalle esposizioni a campi elettrici, magnetici ed elettromagnetici") rules for electromagnetic exposure which are more strict than the European one.

EAS and RFID systems, working at low frequencies (less than 10 MHz), produce fields with negligible propagating features. The exposure of people is therefore limited to the EM field in the close proximity to the reader and its intensity attenuates very fast as soon as the distance grows. In this condition, if there is more than a single reader, it is reasonable to consider the exposure induced by each reader a time.

The systems working at the range of 300 MHz - 3 GHz emit microwave. In this case a true propagation phenomenon have to be considered verifying the threshold of exposure even at some meters from the reader.

The particular exposure to electromagnetic (EM) fields caused by EAS and RFID systems depends on different spatial and temporal characteristics of emission (frequency, power, modulation) and on typology and installation of device.

The first reported example, taken from the open scientific literature [5],[6], refers to an anti-theft gate operating at 30kHz. It is possible to consider the gate as two rectangular coils, partially overlapped with 100A in-phase currents (fig. 1).

The anatomic model of human body adopted for the dosimetric evaluations has a resolution of 1.974x1.974x2.93 mm and refers to an adult man. Starting from this geometry, it was possible to derive other models for children of 10 -and 5-years old (fig. 2).

By evaluating the current on the coil, and, applying the Biot-Savart law, the magnetic flux density B has been obtained in the absence the human body. Computed magnetic flux density at different heights from the floor has revealed that the field is much higher in the case of the children (4-5 times for the 5-years old model and 2-3 times for the 10-years old one) with respect the adult configuration. In any case the magnetic flux density exceeds the limit established by ICNIRP of 6.25 μ T for general public exposure.

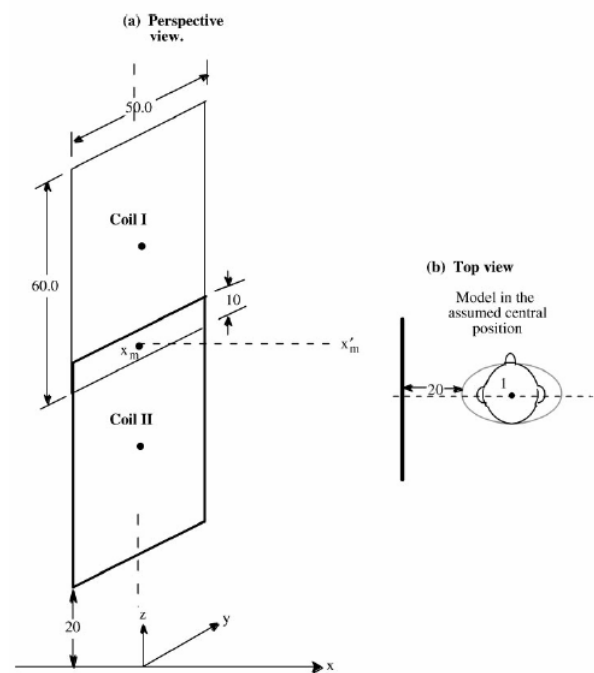


Figure 1: (left) of EAS gate model employing two coils. Sizes are expressed in centimetres. (Right) gate-human body mutual position. The

distance between gate and shoulder is 20 cm.

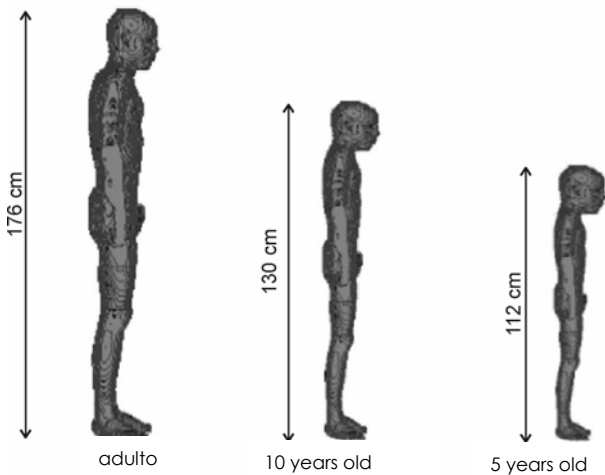


Figure 2: three anatomic models used to calculate the induced electric field and the density of current caused by the exposition to electromagnetic fields of low frequency.

The values of current and electric fields in the different organs of the three models can be compared directly with the based restriction. In the adult anatomic model the levels in brain and in spinal cord are very low compared with the ICNIRP values for non controlled exposure of the people (for 30 kHz the maximum density current admitted is 60 mA/m²).

For children models, the maximum values in brain are very close to the ICNIRP threshold (64.6 mA/m², child 10 years old) or more (98.9 mA/m², child 5 years old). So, while the magnetic flux density values are 5 times over the threshold the derived reference levels, in the case of basic restriction the values are about 60% over the allowed values.

Let's examine the case of Rfid system of UHF frequency 860-960 MHz .

To estimate the levels of SAR in the human body exposed to irradiation from an Rfid station, a realistic map of then human body (Visible Human Project [7]) has been built. The model has 4mm×4mm×4mm resolution and includes head, chest and more that 40 tissues. In this scenario the EM field has been modelled very simply, without considering, for example, the features of the transmitting antenna, the type of modulation, the interaction with the environment (floor and ceiling) and the indoor furniture that generally

modify the distribution of the field. Even in these simplified hypothesis, the results could be a preliminary reference for the distribution of SAR in a EM field.

The EM field, which propagates toward the human body at distance d from the emitting reader, can be simply expressed, within the previous free-space assumption, in terms of the power radiated by the antenna as $|E| = \sqrt{120EIRP} / d$, where EIRP is the Effective Isotropic Radiated Power of the reader. The power absorbed by human body has been then evaluated by means of an electromagnetic simulator based on the FDTD (Finite Difference Time Domain) method [8], [9] assuming a transmitted power 3.2W (EIRP) (2W ERP Effective Radiated Power). This value corresponds to the maximum value allowed by European regulations for this class of devices.

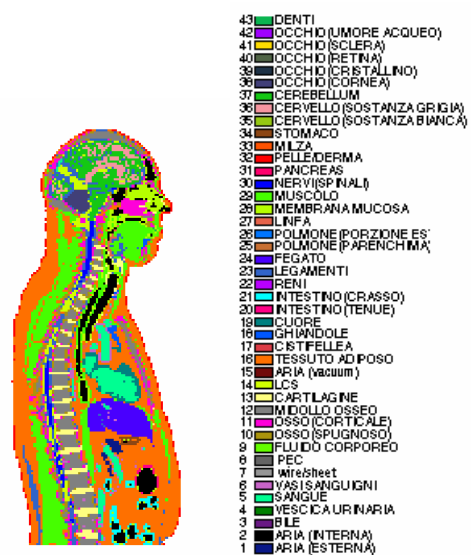
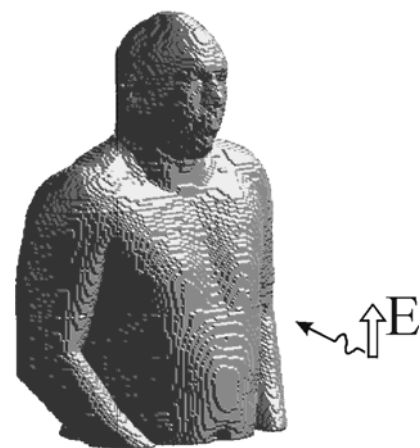


Figure 3: Anatomical map of an adult with a 4mm×4mm×4mm resolution. The model is irradiated by a plane wave coming from the reader, for instance placed onto a wall. The

white arrow indicates the polarization of the incident electric field.

Table below resumes the maximum values of electric field and SAR in the head, in the trunk and the mean value of SAR in the full body at 900MHz. The SAR calculation is expected to be accurate for a body-reader distance larger than 0.5m. These values must be compared with the data prescribed by the mentioned law.

Table VIII: values of EM field without human body and values of SAR calculated in the realistic model of the human body at the different distances from source. Data referred to frequency of 900 MHz.

d [m]	Unperturbed r.m.s. E [V/m]	Localized SAR in the head [mW/kg]	Localized SAR in the trunk [mW/kg]	Body averaged SAR [mW/kg]
0.1	98	-	-	-
0.2	49	-	-	-
0.5	20	13	8	6
1.0	10	3	2	1.5
2.0	5	1	1	<1
3.0	3	<1	<1	<1
4.0	2	<1	<1	<1

The comparison has been conducted with respect to the Italian regulation, that is more restrictive than European one.

The intensity of electric field is less than 20 V/m when the distance between body (or part of body) and the source is more than 0.5m. The intensity is less than 6 V/m for distance major or equal to 2m.

If we consider the basic restrictions on the SAR in the case of generic population, a true conservative safety distance could be 0.5 m, after which the estimated SAR is an order of magnitude smaller than the prescribed limit of 0.08 W/kg.

To sum up, even if we have analysed the model without considering the modulation and in the worst hypothesis of a continuative exposure, the minimum safety distance between the human body and the reader is about a fraction of meter.

The European and Italian law about the safeguard of RFID and EAS obliges the RFID

and EAS producers to be compliant to the mentioned prescriptions.

The producer is not aware of the levels of exposure where the devices will operate. In addition there are no regulations concerning the compliance evaluation following to the installation of the device.

Much more case studies on typical scenarios are however required to assess a comprehensive knowledge base useful to the manufacturer and the installer of the device to avoid or reduce the site-specific computer simulation or measurements.

References:

[1] Working group CNIPA-Politecnico di Milano according to the agreement stipulated 18th April 2006.

[2] Working group CNIPA - Politecnico di Milano - Biblioteca Centrale, Facoltà di Economia dell'Università degli Studi di Torino, as instance of the agreement [1].

[3] Working group CNIPA-Politecnico di Milano-Ministero dei Beni e delle Attività Culturali, as instance of the agreement [1].

[4] Working group CNIPA-Politecnico di Milano-Agenzia delle Dogane, as instance of the agreement [1].

[5] O.P. Gandhi, "Electromagnetic fields: human safety issues", Annu. Rev. Biomed. Eng., Vol.4, pp.211-234, 2002

[6] J.F. DeFord, O.P. Gandhi, "An impedante method to calculate currents in biological bodies exposed to quasi-static electromagnetic fields", IEEE Transaction on Electromagnetic Compatibility, N.27 pp.168-173, 1985

[7] M. J. Ackerman, "The visible human project: a resource for education", J. Acad. Med. N.74, pp. 667-670, 1999

[8] G. Marrocco, F. Bardati, "BEST: a finite-difference solver for time electromagnetics", Simulation Practice Theory ,vol. 7, pp. 279-293, Jul. 1999.

[9] G. Marrocco, "Body-matched antennas for wireless biometry", Proceedings of The European Conference on Antennas and Propagation: EuCAP 2006, pag.795