RFID implants: opportunities and challenges in the identification and authentication of people

Paweł Rotter[1, 2], Barbara Daskala[3], Ramón Compañó[1]

[1]European Commission, Joint Research Centre,
Institute for Prospective Technological Studies (IPTS)*
{pawel.rotter, ramon.compano}@ec.europa.eu

[2] On leave from: Automatics Department,
AGH-University of Science and Technology in Kraków, Poland

[3]European Network and Information Security Agency (ENISA) †
barbara.daskala@enisa.europa.eu

1. Introduction

1.1 Identification and authentication of people: established technologies

Information and communication technologies (ICT), in general, and the Internet, in particular, have led to a 'digitalisation' of information and to 'always-on' remotely accessible services. To ensure that these services are accessed with appropriate levels of security and privacy, the need for the identification and authentication (I&A) of individuals has increased. For most applications, the I&A process is the first line of defence, which aims to prevent unauthorized access to computer systems [1]. *Identification* is the means by which a user provides a claimed identity to the system, while *authentication* relates to the verification of that person's identity, i.e. it ensures that a person is who he/she claims to be [2].

I&A methods can be clustered in three main groups:[1]

- Something the individual *knows* (e.g. a password or Personal Identification Number (PIN)). Passwords and PINs are usually used in combination with user IDs and allow I&A in a single process. Simplicity and affordable operational costs have contributed to a wide diffusion of this method. A drawback to authentication by 'something you know' is the way users manage their passwords, often sharing them or keeping them in an unprotected way (e.g. in post-it notes on computer screens), which invalidates security. In addition, passwords can be obtained through cracking,[2] eavesdropping[3] or social engineering.[4]
- Something the individual *has* (using a token, e.g. a smart card). Token-based systems – similar to PIN based ones – are quick and convenient. Tokens may have the form of contact smart cards or may be contact-less. The latter have become increasingly popular over the last

* The views expressed in this publication are purely those of the authors and may not in any circumstances be regarded as stating an official position of the European Commission.

† The views expressed in this publication are purely those of the author and may not in any circumstances be regarded as stating an official position of the European Network and Information Security Agency.

decade because of the extra convenience. However, the need for a physical medium with particular interfaces makes this technology, in general, more expensive than passwords.

- Something the individual *is*. Biometric technologies make use of people's physical traits such as fingerprints, iris patterns, face images or behavioural characteristics, like signatures or their way of walking. In principle, well-implemented biometrics can be considered as a reliable method for authenticating people. Nevertheless, the statistical nature of biometric matching, the relatively high cost of efficient biometric-based identification systems and their low social acceptance are barriers to wider deployment.

Each of these methods can be either employed alone (one-factor authentication) or in combination (multi-factor authentication) to provide more reliable verification of identity.

1.2 Radio Frequency Identification technology

Radio Frequency IDentification (RFID) technology was originally developed for automatic identification of physical objects [3], [4]. An RFID tag is a small device, attached to an object, which emits an identification signal through radio waves in response to a query by an RFID reader. This information is captured by the reader and then further processed. RFID tags are already employed as barcode replacements offering several advantages. Unlike printed barcodes, RFID tags do not require line-of-sight during their reading. This allows multiple scanning (e.g. scanning the whole content of a truck or shopping basket) and enables further automation of many industrial processes. In addition, RFID tags may contain data other than the unique identification number, such as information on product details or, if combined with sensors, the history of storing conditions (e.g. temperature, humidity or any falls or shocks the product may suffer). Therefore RFID tags are increasingly used in production and the logistics chain of enterprises [5]. Additionally, RFID technology is starting to penetrate the medical and healthcare sector, defence, agriculture and other domains [6]. Both industry and governments are strong promoters of RFID technology.

RFID tags for the I&A of people have already been introduced. All EU Member States, the US and many other countries are gradually deploying electronic passports. These passports contain RFID tags that store personal data, including the owners' biometrics. This allows for semi-automatic authentication of people at borders. Credit-card-sized contactless smart cards, based on RFID technology (like Mifare, www.mifare.net), are also becoming increasingly popular for access control. While some RFID-enhanced smart cards contain only identification numbers, others include additional cryptographic security features to protect the data during transmission. More sophisticated RFID-based devices not only identify, but also can track people's location and activities [7].

1.3 RFID implants

RFID implants are introduced into the human body. In this paper, we will focus exclusively on passive implantable RFID tags that are not connected to the neural system. These devices are already commercialised and are specifically designed to facilitate the I&A process.

In October 2004, the first RFID implant – the so-called VeriChip – obtained approval from the US Food and Drug Administration [8]. The VeriChip implant, which stores an identification number only, can be read from a distance of up to 10-15 cm.[5] The ID number is long enough to identify uniquely everybody in the world. Other data related to the owner are not stored in the RFID implant itself, but in a centralized database. The first commercial application, called VeriMed, is designed to identify patients in healthcare (see Section 3.5). An authorized doctor can

access a patient's medical files through a password-protected website, based on the patient's ID number detected by an RFID reader.

RFID implants are passive tags, i.e. that they do not require batteries to operate but make use of the energy emitted by an external RFID reader. As a result, once implanted under the skin, they can be operational for many years. Their extremely small size and lack of an internal power source limit the devices' performance in terms of memory, processing power and communication range. The hardware limitations make it difficult to design RFID implants with advanced authentication methods. The limited communication range makes it difficult to interoperate with other information technologies like Bluetooth, GPS, etc. However, this limit can also be seen as an advantage from a security and privacy point of view.

In the following section, we present opportunities and challenges of RFID implant technology in comparison with other established I&A technologies. In Section 3, we propose some emerging applications for RFID implants.

2. RFID implants vs. established identification and authentication technologies – opportunities and challenges

As RFID implants are a new technology, the advantages and risks stemming from its use are not yet fully understood. In the following, we present a general overview of the opportunities and challenges as they appear today. This overview is not intended to be complete or exhaustive.

2.1 Advantages to using RFID implants as identification and authentication technologies

The use of RFID implants for the I&A of people provides some advantages compared to established methods. The identification process is fully *automatic* and promises to be more *convenient*. The user is not required to take any action;[6] there is no need to type or confirm any information or to carry any token. The user does not have to have clean hands, as he would when using a fingerprint scanner, or to stand still without blinking, as he would have to when having an iris image captured. I&A with RFID implant is practically *immediate*, whereas with other technologies time is required for typing passwords (often also for searching for them and retrieving them), for acquiring and matching of biometrics or for taking a smart card out of a wallet.

Implants are a *reliable* method of identification, especially when compared to biometrics, which due to the statistical nature of their matching process do not guarantee 100% error-free results.

Implants are more *durable* than tokens and many types of biometrics, which usually change during a person's lifetime. Unlike tokens, implants cannot be lost or stolen unless an attacker physically assaults a user to extract the implant.

RFID implants *can be used by everyone* without exception, including people with cognitive impairment, if they are willing to accept the implant. The user will be always identifiable, even if he/she is unconscious or not carrying any identity documents.

2.2 Concerns and challenges regarding RFID implants

Despite these advantages, there are serious concerns regarding the adoption and use of the RFID implants. In this section, we survey several concerns, mainly related to technical security, privacy, ethical social, and health issues.

Technical security issues

The permanent and physical link between an RFID tag and a person makes RFID implants more susceptible to privacy risks than any other kind of contactless tokens [9]. A major fear relates to the loss of privacy through being identified without one's consent or awareness. Despite the short communication range of today's RFID implants, there is a risk that they may be misused for the physical *tracking* of a person. Placing readers at both sides of door frames would enable the detection of implants in users' arms and capturing the stored information without the consent or even the awareness of the users.[7]

The use of RFID implants for authentication brings a particular risk related to a *coercive attack,* when an attacker forces an authorised user to provide his/her credentials. Such a security threat may occur for any I&A method, but for RFID implants it carries the risk of physical harm, as an attacker could cause injuries by extracting the implant from the victim's body. Therefore, it has been argued that RFID implants may be appropriate for identification of people but, regardless of any future development of technical security solutions, they cannot provide secure authentication. Some argue further that they should be designed to be easy to clone, in order to make their extraction by an attacker unnecessary [10].[8] However, ease of cloning reduces the reliability of the identification.

Another kind of threat is that of the unauthorized replication of information on a RFID tag which may lead to a *replay attack*, i.e. repeating the same authentication sequence as the one provided by an authorized person and thus stealing another person's identity. Also, currently deployed RFID implants do not yet include options for advanced encryption or tag authentication through a challenge-response protocol, which would counter the replay attack technique[9].

In addition, RFID implants bear a number of other security risks related to RFID systems in general, like: eavesdropping of data exchanged between tags and readers, men-in-the-middle attack, duplication of the authorized person's tag or attack on system's backend – databases, which in this case contain personal and often sensitive information [9].

Privacy and Ethical considerations

The European Group on Ethics in Science and New Technologies (EGE) recently published their opinion on the use of ICT implants, where ethical and privacy considerations are presented [11]. EGE states that –although implants may at first seem ethically unproblematic– they may pose a risk to human dignity by not respecting the autonomy and rights of individuals. In general, technologies that enable the tracing of the movements and habits of individuals "would be bound to modify the meaning and contents of individuals' autonomy and to affect their dignity" [11]. RFID implants potentially enable a permanent and/or occasional tracking and location of people. The EGE report notes that there should be protection against intrusion into one's private sphere and confers "the right of informational self-determination on each individual – including the right to remain master of the data concerning him or her" [11].

Tracking people or accessing their data remotely has an economic dimension. These data could be used for profiling and analysis of consumer behaviour. While businesses may use this to offer personalized services, there would be a risk of misuse., These privacy concerns pose the question of whether there are legal gaps and whether current legislation on data protection need to be reconsidered, as has been the case with other emerging technologies and applications [12].

Health issues

Potential medical risks have been analysed by the US Food and Drug Administration (FDA). The FDA approved the commercialisation of VeriChip implants, though it points to some potential

risks: “adverse tissue reaction; migration of the implanted transponder (…), failure of implanted transponder; failure of inserter; failure of electronic scanner; electromagnetic interference; electrical hazards; magnetic resonance imaging incompatibility; and needle stick” [13].

In September 2007, the Associated Press reported on studies, dating from 1990s, claiming frequent cases of cancer among laboratory rodents injected with RFID implants [14]. The reports were reviewed for the Associated Press by leading cancer specialists, who concluded that these results do not necessarily imply that RFID implants cause cancer among humans. A similar view is given in [15]. A main argument is that tumours in laboratory rodents can be caused by the process of injection rather than by the implant itself. Apparently there is a different, more sensitive body reaction when rodents are injected than other beings. This could explain why millions of dogs and cats have been chipped and only one case of cancer by the side of the microchip implant has been found during the past 15 years (although there might be more, not reported). 2,000 people have been injected so far and no health problems related to the implants have been reported.

At the moment, it is still uncertain whether RFID implants may cause cancer. Although the probability of getting cancer may be low, the potential risk understandably makes people nervous about implants.

Low social acceptance

Identification technologies generally have a low acceptance rate, and recent studies has shown acceptance rates especially low for RFID implants [16]. In a study commissioned by the New Jersey Institute of Technology (NJIT) in 2002, 78.3% of respondents said they would not be willing to implant a chip in their body. Similarly, a study by the consultancy firm CapGemini in 2005 reveals that the percentage of people “not at all and somewhat unwilling” was between 42 and 55%, while those that were “very and somewhat willing” was between 31% and 44% (dependently on the application). In a recent poll (“Live vote”) at the MSNBC site, 66% of the respondents replied “no way” to the question “would you like to be chipped?” (see: www.msnbc.msn.com/id/5439055/). Interestingly, 27% replied positively saying they would accept “if there was a good reason”. The results of another MSNBC survey performed after the publication of potential cancer risks related to RFID implants were even more negative: 83% of responders said “No way...”, 6.8% said “Of course. It’s worth the risk...”; and the remaining 10% were “not sure” (www.msnbc.msn.com/id/20648530). Although these surveys are not comparable (different conditions and target groups), they have in common a high rejection rate of implanted chips. Implanting an RFID tag is considered intrusive and ”creepy” (although placing the chip with a syringe is not considered surgery) and many people are reluctant to have this done.

2.3 Some economic considerations

Given that the commercialization of RFID implants is recent and the business model is not yet mature, any statement on future markets has to be made with care. Installing an RFID implant system for I&A in a given environment, like the workplace, is currently more costly than alternative I&A systems, possibly with the exception of some high-security solutions; e.g. some biometric implementations require expensive scanners and software. In the first phase of a system’s deployment, investments in infrastructure (readers, backend, and system integration) are required. Once the infrastructure is established, maintenance costs are low and the overall costs are mainly related to enrolment of new users. At the moment, $150-$200 has to be spent for each VeriChip implant, including the insertion procedure. This is more expensive than other I&A technologies, such as tokens, but is expected to decrease in the future. If many people decide to

use RFID implants, they may benefit from economies of scale. However, whether lower production costs will imply lower prices for customers is still unclear, as, for the moment, VeriChip is the only provider of RFID implants approved for commercial use.

3. Application fields for RFID implants

The major driver for RFID implant deployment is the automation of the I&A process. It makes existing services more convenient and will enable further services; these new services may in turn provide value through higher personalisation. In this case, RFID implants' feature of fully-automated identification and continuous detection of a person's presence is a valuable asset.

The adoption of RFID implants will mostly depend on the security requirements of the environments in which they are deployed. Based on this criterion, we will categorise and then examine the potential applications of RFID implants.

a. applications *without strong security requirements* (Sec. 3.1)
b. secure environments, where additional security is provided at the entrance to a physically restricted area (Sec. 3.2)
c. non-secure environments, when they may enhance security and convenience in combination with other I&A methods (Sec. 3.3)
d. mobile devices and services (Sec. 3.4), which can be used both in secure and non-secure environment.

Section 3.5 is dedicated to the *healthcare sector*, which combines all three environments listed in points b, c and d (secure, non-secure and on-the-move). Moreover, healthcare is the first area where RFID implants have already been deployed and are expected to play an important role in the future. Intelligent homes and cars are discussed in Section 3.6 as examples of secure *smart environments* of the future. In Section 3.7, we make some assumptions on other applications of RFID implants which may emerge in a longer-term perspective. Finally, in Section 3.8 we compare the prospects for expansion of the discussed applications.

3.1 Applications not requiring strong security

Applications under this category are those which require the identification of users but strong measures against identity theft are not necessary. Here, RFID implants may replace other technologies simply because they are more convenient, as identification through the implant is immediate, does not require any action from the user and the implant cannot be forgotten, lost or accidentally destroyed. Examples include the Baja Beach Club in Barcelona, where club members who have an RFID chip implanted benefit from a quicker service, as drinks are automatically charged to their bank account, and they thus get more personalized service, as their consumption habits are recorded. The club's owners have expanded the RFID implant programme to a bar they own in the Netherlands.

Apart from these VIP clubs, the use of RFID implants for non-secure applications has hardly spread in our society. It seems that the advantages gained do not outweigh the ethical, privacy and health concerns.

3.2 Identification and authentication in secure environments

In restricted workplaces, the identity of employees is verified at the entrance and strong authentication of people who are already inside is usually not necessary. In such situations, RFID implants can help prevent authorized people from providing credentials to unauthorised users. In

highly protected environments where security concerns prevail over privacy (e.g. nuclear power stations) implant-based systems could also facilitate continuous monitoring of the location of workers. For instance, employees' movements from one room to another could be tracked by placing RFID readers in all doorways, so in the case of an accident, location of every worker is known. RFID implants may also be used in secure, but more open environments like hospitals. They would help to prevent access by unauthorized people to certain instruments, restricted places, or to patients' medical files. In such environments, RFID implants facilitate the identification of a person. Where strong authentication is required, RFID implants can be complemented with other I&A technologies, like PINs/passwords, tokens and/or biometrics.

For example, in 2004, more than 100 employees in the organised-crime division of the Mexican Attorney-General's offices received implants giving them access to restricted areas [17]. In 2006, an Ohio-based company had chips embedded into some of its employees. CityWatcher.com, a private video surveillance company, uses the technology for controlling access to a room where it holds security video footage for government agencies and the police [18].

3.3 Identification and authentication in non-secure environments

RFID implants in combination with established I&A technologies can provide additional security. They could protect systems from accepting PINs/passwords obtained by theft, or which have been cracked or disclosed without authorisation. Similarly, the RFID implants may reduce the risk of false authentication with a stolen token or with one which has been loaned by an authorized person to a third party, either willingly or as a result of blackmail. Prominent application fields are those where people are less willing to delegate their rights, e.g. withdrawing cash at an automatic teller machine.

An identification number read from an RFID implant may also be used to speed the process of biometric identification. To identify a person, his/her biometric sample must be compared with each sample in a database. The RFID implant could speed the process by yielding an immediate and reliable identification (1:N), while biometrics would offer a strong authentication (comparing the user's sample with only one database entry, indicated by the RFID implant).

Finally, as mentioned in [16], it is possible to deploy RFID implants which would incorporate some biometric information, so the user and implant may authenticate each other mutually. It would be would secure against a coercive attack as an implant extracted from victim's body could not be used by other person (who has different biometric features). However, it would be still possible that an attacker can duplicate the identification number and modify biometric features. Moreover, it would raise a risk of copying the biometric features by a potential attacker.

3.4 Access control for mobile devices and services

Mobile devices, like portable computers, PDAs or mobile phones, store a growing amount of confidential information about their owners, and people are motivated to secure them. In existing devices, people are usually identified when they switch on the device. When a user leaves, the device still retains the authentication for a certain time period, during which an unauthorised person could get access. An RFID-based system can detect continuously the presence of the authorized person and demand a re-authentication when this person leaves the area. For high-security applications, the mobile device would identify a person by reading his/her RFID implant, and then the owner would authenticate to the device via a PIN/password or biometrics.

The 'smart weapon' is another example where the application of RFID implants can increase the security of a mobile artefact. On 14 April 2004, VeriChip, announced a partnership with gun maker FN Manufacturing to produce a police gun with an RFID reader embedded, so that the gun

cannot be fired should it fall into the wrong hands. A digital signal unlocks the trigger when the scanning device inside a handgun identifies the authorized police officer; otherwise the gun is useless [19]. Some critics worry that malfunctions in this system may render the gun useless in emergency situations.

3.5 Identification in healthcare

In the healthcare sector, RFID implants might offer advantages for both medical personnel and patients. Vital information can be easily and immediately retrieved everywhere, even in cases where patients are unconscious.

The first commercial application, VeriMed – a system for patient identification and heath-care flow management – has been adopted by a number of hospitals (620 in July 2007, [8]). The system is especially recommended for people who suffer from cognitive impairment, such as Alzheimer's disease, or diseases which put them at high risk in an emergency situation when instant identification of unconscious patients is crucial. On 7 August 2006, the first known life-saving incident involving a VeriChip was reported. A VeriChip subscriber, was rushed to a medical center with head trauma following a crash during a high-speed police pursuit. Doctors accessed his medical records in the VeriMed database, using the ID retrieved from his implant [8].

The highest acceptance of any RFID implant application is for lifesaving purposes. According to the Cap Gemini survey, the percentage of people saying "not at all & somewhat unwilling" and "very & somewhat willing" for lifesaving was 42% and 44% respectively, the same for using of biometrics for passenger identification in air travel, which is already in place.

3.6 Smart environments

The Ambient Intelligence (AmI) vision assumes that people will be surrounded by intelligent interfaces embedded in a range of objects. These smart environments will respond to individuals in an unobtrusive way [20]. RFID implants could provide the interface between people and the smart environments. For example, an RFID reader in a car would read a person's ID, recognize that he/she has permission to drive the car, open the door, adapt the seat height and positions the mirrors.[10] Similar applications could use RFID in smart homes.

Some people have volunteered to have RFID tags implanted to experience ambient intelligence environments. Prof. K. Warwick's RFID chip allows a computer equipped with a reader to detect his presence at the Cybernetics Department of Reading University. It automatically opens doors, and switches lights, heaters and computers on and off [22]. Similarly, an entrepreneur A. Graafstra has an RFID chip implanted in each of his palms. The chips were originally manufactured for industry or supply chain purposes and one of them was equipped with crypto-security features. Graafstra uses his implants to open the front door of his house, start his car and log on to his computer [23].

3.7 Other potential long-term applications

Up to now, the main purpose of wireless-based networks was communication, but recently the network data is increasingly used to provide location-based services. Examples of location-based services include emergency services (e.g., location of emergency calls by the fire brigade) or local information services (e.g., finding the nearest ATM.). The communication range of RFID implants is limited to about 0.5 m (10-15 cm with a hand reader), but an intermediate device, e.g. a mobile phone equipped with an RFID reader, could provide a connection between the RFID

implant and the network. The user would activate the interface device, e.g. a phone, to request a service via the wireless network and the RFID implant would provide the user's identification. In the long term, if a dense network of RFID readers were available, no 'bridging device' would be necessary. Thus, combining RFID implants with *location-based systems* may deliver new personalised services for people on the move. At the same time of course, it may lead into an Owerlian nightmare, where individuals are constantly tracked.

3.8 A comparative outlook

Forecasting the deployment of RFID implants must take into account several factors at the same time, including technical, market, social and ethical considerations. Credibility of such a forecast is limited because many of these factors are uncertain, like future attitudes of society or health-related issues. RFID implants are already used in healthcare, low-security systems and secure environments, while – to the best of our knowledge – there are no examples yet where this technology is used in mobile devices, non-secure environments, or intelligent homes.

A commercial system has already been developed for the *healthcare sector*. According to VeriMed's company information, the market is growing fast [8]. However, the number of subscribed hospitals and practitioners is still tiny is absolute terms. People may be tempted to accept RFID implants if they are convinced that these could help to save their lives in emergencies or enable access to better healthcare. Benefits from instant identification of patients and access to their medical files anytime and anywhere are numerous and they might increase with the growing mobility of society. RFID implants could become a mass market even if a small only a fraction of the population would subscribe[11]. If patients do not accept RFID implants, however, only organic growth will be possible.

The first RFID implant applications in *low-security systems* emerged almost at the same time as they did in healthcare, but have not expanded significantly since then. We think that only a limited group of people would be willing to get an implant simply for convenience or entertainment purposes. For such purposes, other alternatives, like contactless smart card, ornament tokens on chains, rings, or embedded in watches, appear to be more attractive. We do not see any indication why this attitude might substantially change in the future, therefore it seems unlikely that RFID implants will become popular in this area.

RFID implants might play a role in I&A in *secure environments*, especially at the workplace, enhancing security, efficiency and convenience. However, only a small fraction of the population works in highly secure environments. In addition, as employers cannot force employees to implant RFID tags, this must occur on a voluntary basis only. If only some of the staff accept them, the benefits will be much smaller.

We consider that there is potential to use RFID implants for activating *mobile devices*. Although no such application has yet been reported, it would be easy to implement if there was a demand. It would only require embedding an RFID reader into the mobile device. As a first step, RFID implants can serve to secure access to mobile phones, PDAs or laptops but in the future they could also be used to identify the user in order to supply him/her with personalized services, other than those authenticated by the SIM. The number of mobile devices is huge and if only a small fraction of people use it, this could result in a large market.

In *non-secure environments*, RFID implants need to be combined with other I&A methods to increase the overall security of the system. However, including implants into such systems requires adaptation of the infrastructure, e.g. building RFID readers into cash machines. Using RFID implants in this area is certainly possible, but they would have to compete with biometric technologies, which are generally more secure and have higher social acceptance.

A “smart” environment is probably a longest-term application for RFID implants. However, it is likely that interfaces, other than RFID implants, between people and the “smart” environment will be tested first. Moreover, the concerns that widely-diffused intelligent machines will take part of the control over everyday decisions must be dealt with.

When discussing deployment prospects it is important to note that applications are mutually reinforcing; the use of RFID implants in one application will enable their diffusion in another field. There is no need to get a different RFID tag implanted for each application, as one implant may be used for several I&A-based applications. This scenario, however, would require a compatible standard across applications. Whoever has an RFID implant for healthcare purposes, and has had a good experience, may possibly be tempted to use the same ID number for other purposes. In view of this dependency, successful use in a given domain may trigger other applications. Therefore, the healthcare domain is a test-bed for social acceptance of RFID applications as a whole. Should it remain a niche market in the medical sector, then it is unlikely to succeed anywhere else.

4. Conclusions

The first commercial RFID implant applications already exist, the best known being the VeriMed system for identifying patients in healthcare. Benefits may be considerable, both in economic and service terms, if fundamental security measures for personal data treatments are respected, and if related services are offered on a large scale. In our opinion, medical applications will play a pivotal role for the whole domain; if RFID implants get established in healthcare, then – at a later stage – other applications may emerge. Examples include protection against unauthorized access to personal devices, like mobile phones, PDAs or computers, access control where security requirements are low (like sport clubs, or cafeterias) or access control in closed areas (e.g. the workplace) where implants protect only against unauthorized access by a colleague. A couple of VIP clubs have already introduced RFID implants for their clients, some companies have provided their employees with such devices, and others may follow. However, when high security standards have to be guaranteed, RFID implants must be complemented with additional measures. Under these circumstances, RFID implants may also be employed as one of the elements of a high security system, increasing the convenience and security of the overall system.

Considering the issue of low social acceptance, we could argue that it is also a challenge for other I&A methods, such as biometrics. Some types of biometrics are not accepted by large parts of society. For example, fingerprints are still associated with criminal applications in many cultures and some people perceive iris scans as invasive. However, in the recent past, some technologies have moved from low social acceptance into much higher acceptance. One such technology is in-vitro fertilisation, which is now widely accepted, although it faced huge opposition only a couple of decades ago. It is possible that a significant part of society might accept RFID implants in the future, if the benefits are clear and outweigh the perceived threats. Indeed, recent polls indicate the high importance of convenience for consumers and increasing concerns about potential threats

related to terrorism [16]. Two ideas for improving implanted RFIDs are to make implants removable and to allow users to deactivate their implant. Both these ideas would dramatically changes both advantages and disadvantages of the technology.

Not everything that is technically possibly should automatically be ethically admissible, socially acceptable and legally approved. RFID implants bring with them many medical, ethical and privacy concerns which cannot be ignored. Addressing these concerns appropriately may improve and boost citizens' trust in RFID implants and ensure a more favourable social acceptance rate. However, increasing the social acceptance rate should not be an immediate goal for two reasons. First, it is important at this stage to consider and evaluate adequately the specific risks that this new technology entails. Secondly, wider adoption of RFID implants does not depend on increasing social acceptance alone. There are other factors that will also affect the future of this technology, such as economic and legislative factors.

It would be beneficial to carry out a careful impact assessment, which systematically identifies the risks that RFID implants pose for ethical values, privacy, health and economic aspects. The impact analysis would give an indication of whether, and ***in which cases,*** RFID implants should be used. As the EGE report points out, identifying the acceptable risk threshold with regard to the values at stake should be the aim of the risk management actions. Given that the technology is new and we have yet to evaluate all the risks it entails, we should adopt the "precautionary principle".[12]

It must be ensured that the application of RFID implants does not violate human rights. Individuals are entitled to live with dignity and to have full control over their physical bodies as well as their personal data. Therefore, as a minimum, within the foreseeable future, the informed consent of the individual must be obtained, and individuals must be allowed to opt-out, i.e. not be implanted. This will complicate many possible application of implanted RFIDs, but it is our judgment that the informed consent is more important than the rapid deployment of implanted RFIDs.

RFID implant-based applications for I&A are still in their infancy. Although quantifying their real benefits still needs in-field testing, there are some indications of economic and social potential. On the other hand, today's commercial RFID implants do not offer sufficient support for security of data and protection of privacy. This, together with concerns about health and ethical issues, is a significant obstacle for further deployment. Nevertheless, technological performance and user acceptance may change in the future and a wide use of RFID implants for I&A in a number of applications is possible. Each of these applications will have to be judged carefully for its costs and benefits to society and individuals.

Acknowledgments

The authors would like to thank IPTS staff Ioannis Maghiros for his many helpful comments and suggestions and Patricia Farrer for her help with preparation of the manuscript.

This work has been done within EU research project FIDIS (Future of IDentity in the Information Society, www.fidis.net).

References

[1] National Institute of Standards and Technology (NIST) U.S. Department of Commerce (1995) *An Introduction to Computer Security: The NIST Handbook*. Special Publication 800-12, October 1995.

[2] S. Hansche, J. Berti and C. Hare (2004) *Official (ISC)²® Guide to the CISSP® Exam*. Auerbach Publications

[3] S. Garfinkel and B. Rosenberg "RFID: Applications, Security, and Privacy". Addison-Wesley Professional, July 2005.

[4] I. Maghiros, P. Rotter and M. van Lieshout (editors) *RFID Technologies: Emerging Issues, Challenges and Policy Options*. EUR IPTS report, 22770 EN, Sevilla 2007, available at: http://www.jrc.es/publications/pub.cfm?id=1476

[5] I. Bose and R. Pal "Auto-ID: managing anything, anywhere, anytime in the supply chain" Communications of the ACM, Vol. 48, no. 8, August 2005, pp. 100-106.

[6] B. Nath, F. Reynolds and R. Want "RFID Technology and Applications." Pervasive computing, January-March 2006, Vol. 5, No. 1

[7] J.R. Smith, et al. "RFID-based techniques for human-activity detection" Communications of the ACM, Vol. 48, no. 9, September 2005 (Special issue on RFID), pp. 39 - 44

[8] VeriMed website: http://www.verimedinfo.com

[9] P. Rotter *A Framework for Assessing RFID System Security and Privacy Risks*. IEEE Pervasive Computing, Vol. 7, no. 2, April-June 2008, pp. 70-77.

[10] J. Halamka, et al. "The Security Implications of VeriChip Cloning." Manuscript in submission, March 2006. Available at: http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/verichip/Verichip.pdf

[11] European Group on Ethics "Ethical aspects of ICT implants in the human body." Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, 2005. Rapporteurs: S. Rodota and R. Capurro.

[12] B. Daskala, I. Maghiros "D1gital Territ0ries – Towards the protections of public and private space in a digital and Ambient Intelligence environment", EUR 22765EN, IPTS, European Commission

[13] "Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information." U.S. Department of Health and Human Services, Food and Drug Administration, Center for Devices and Radiological Health, December 10, 2004, http://www.fda.gov/cdrh/ode/guidance/1541.pdf

[14] T. Lewan "Chip Implants Lined to Animal Tumors". Associated Press, 8 September 2007

[15] W. Wustenberg "Effective Carcinogenicity Assessment of Permanent Implantable Medical Devices: Lessons from 60 years of Research Comparing Rodents with Other Species". 27 September 2007, available at: http://www.verichipcorp.com/files/RodentSarcomagenesis092807Wustenberg.pdf

[16] C. Perakslis, R. Wolk *Social acceptance of RFID as a biometric security method*. IEEE Technology and Society Magazine, Vol. 25, No. 3, pp. 34 – 42, 2006.

[17] "Implantable Chips Get Under Skin of Security Experts". Available at: http://www.adsx.com/newsarticles/01.htm

[18] "US group implants electronic tags in workers" Financial Times, 12 February 2006 available at http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html

[19] "No Chip in Arm, No Shot from Gun". Wired Associated Press , 14 April 2004 , available at www.wired.com/science/discoveries/news/2004/04/63066

[20] ISTAG Reports Grand challenges and Visions for the information society technologies is available at http://cordis.europa.eu/ist/istag.htm

[21] J. Kent "Malaysia car thieves steal finger", BBC News, 31 March 2005, available at: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

[22] What happens when a man is merged with a computer? At Kevin Warwick's webpage, http://www.kevinwarwick.com/Cyborg1.htm

[23] A. Graafstra "RFID Toys" Wiley, 2006.

[24] A. Marburger, et al. "Implantable RFID for The Health Industry" June 2005. Available at: http://www.geocities.com/innovating_competitively/data/Verichip.pdf

[25] Ph. Krauchi, P.A. Wager, M. Eugster, G. Grossmann and L. Hilty *End-of-life impacts of pervasive computing*. IEEE Technology and Society Magazine, Vol. 24, No. 1, pp. 45-53, 2005

[1] Profiling can be regarded as a fourth category of I&A method, where the users are identified and authenticated as belonging to a group with specific characteristics.

[2] E.g. using password-cracking software, like L0phtcrack.

[3] E.g. using of software (sniffers) to monitor packets or wiretapping telecommunication links to read transmitted data [2].

[4] E.g. deceiving users or administrators at the target site [2], using techniques to manipulate them, often without employing any technical computer skills and knowledge.

[5] The VeriChip has been designed to operate at a distance of about 10cm with a handheld reader and 50cm with a door reader but cannot operate at large distances. Simulations (see e.g. Z. Kfir and A. Wool "Picking virtual pockets using relay attacks on contactless smartcard systems.") and practical experiments (see G. Hancke "A Practical Relay Attack on ISO 14443 Proximity Cards.") show that a standard distance can be increased several times (up to 0.5m for standard ISO 14443), but with further increase the signal disappears in the noise of environment. In the supposed case that a reading would be possible at larger distances, there are technologies in place preventing this. One option against relay attack could be a distance bounding protocol, which basically measures the response time of the RFID reader request (see e.g. G.P. Hancke, M.G. Kuhn "An RFID Distance Bounding Protocol").

[6] No user action may also be considered as disadvantage in terms of privacy, as the user may even not be aware of being identified.

[7] 10 cm range of VeriChip implant applies to hand reader. A commercial reader exists (VeriChip Portal Reader), able to scan information from RFID implant of a person passing through the door.

[8] Even in this case, extracting the chip from the carrier may remain easier for some attackers, as cloning it is rather a complicated procedure, requiring specialised equipment and knowledge.

[9] It can be argued that some biometrics are also vulnerable to unauthorised copying (e.g. fingerprints copies can be obtained from a glass, special camera can take high-resolution iris images even from several meters), but having a copy of biometrics usually does not suffice for a replay attack. Security of the modern biometric systems is not based on the biometric data alone, but relies also on a "liveness test", generally integrated in the sensor part.

[10] In the case of anti-theft protection, the risk of coercive attack should be taken into consideration. Some premium car manufacturers were forced to recall from the market a finger print recognition system to open and start a car, after an attempt steal the car of a Malaysian business man. As the thieves were unable to start the engine and drive away, they cut the owner's finger to escape with the car [21].

[11] Marburger at al. [24] foresee that in the next 15 years there will be between 1.0 and 1.4 million VeriMed users world-wide. Unfortunately, the authors do not support their assumptions with a solid analysis, except from a questionable analogy to pet tagging.

[12] For example, in the case of waste management process, precautionary measures have been taken in the form of eco-design and necessary process modifications [25].