Specification Analysis for Secure RFID Implant Systems

Sanaz Rahimi Moosavi[1], Antti Hakkala[1,2], Johanna Isoaho[1], Seppo Virtanen[1], and Jouni Isoaho[1]
[1] Department of Information Technology, University of Turku, 20014 Turku, Finland
[2] Turku Centre for Computer Science TUCS, University of Turku, 20014 Turku, Finland
Email: {saramo, antti.hakkala, johanna.isoaho, seppo.virtanen, jouni.isoaho}@utu.fi

Abstract— **In this paper we derive an engineering specification for functionality, security, and implementation demands for RFID Implantable Medical Devices (IMD) requiring medical data storage and wireless communication. We illustrate the specification by sketching a secure communication protocol for RFID IMDs. The specification follows from our requirements analysis of application characteristics, legal restrictions, security requirements and ethical concerns of IMDs. In our analysis we have recognized three main types of IMD applications: identification, financial and medical/emergency. The hardware implementation constraints and security level requirements of IMD systems differ from mainstream applications of RFID. The presented specification that considers the special operating environment, delicate use cases and safety-critical functionality of IMD systems is aimed to be a conceptual platform for designing robust security schemes and long-term functional and physical reliability.**

Index Terms—**RFID Implant Systems, Security and Privacy, Hardware Limitations, Ethical Concerns, Lightweight Cryptography**

1. Introduction

The developments of mobile and wireless technologies have set the infrastructure for the communication systems universally. Radio Frequency Identification (RFID), one of the recent new wireless technologies, can be used to identify items tagged with an RFID tag. The identification process of RFID is executed by three major modules: an RFID tag, an RFID reader, and a back-end database system. An RFID tag communicates with an RFID reader wirelessly to identify it. The information required to complete the identification process is provided by the back-end database system, which the readers access through the Internet.

Currently RFID technology is deployed in widespread applications, such as electronic passports, asset tracking, toll payments, and entrance access control. RFID tags have for some time been used for identifying animals, and analogous solutions for humans are emerging.

RFID enabled implants are medical devices implanted into a human body through a surgical procedure. One of the prominent implant brands is PositiveID (formerly VeriChip). It was approved by the U.S. Food and Drug Administration (FDA) in 2004 for clinical use [1]. The implant contains only an identification number, and it can be read from a distance of up to 10–15 cm. Other essential data associated to the owner of the tag is kept in a centralized database. VeriMed, the commercial application of VeriChip RFID implants, is designed to be used for patient identification in healthcare.

Like all wireless applications and devices, also RFID is vulnerable to interception or eavesdropping by unauthorized parties. This quite justifiably raises privacy and security concerns. If no countermeasures are in place, it is possible to read some or even all information on an RFID tag without consent, and subsequently acquire relevant information on the item bearing the tag. It is also possible to track an individual tag if its ID is known. Once a tag has been read by an attacker, if the same tag ID is identified later, it is very likely the same tag. This enables location tracking of a previously identified tag. These concerns, while not an exhaustive list, have contributed to RFID technology not being as widespread as it could be. These concerns become more serious when an RFID tag is associated with a human body, either permanently or temporarily.

In this paper we propose security and privacy optimizations for RFID Implantable Medical Devices requiring medical data storage and wireless communication within the boundaries of the tight size, power consumption and processing capability constraints manifested by RFID IMDs. We outline the requirements specification for a communication protocol optimized for this application. The hardware footprint and power consumption limitations and security level requirements of RFID implant systems differ from mainstream applications of RFID due to the delicate use cases and safety-critical specifications. An RFID implant system requires a robust security and privacy scheme to protect the implanted users. We see that communication security solutions being proposed in this regard must be optimized based on characteristic restrictions and requirements of such systems.

A. Related Work

Several communication security schemes have been proposed in literature so far to solve security and privacy issues caused by RFID systems. In the following, we examine some of the most common communication security schemes for general RFID systems.

The *Hash Lock scheme* [2] is one of the easiest security structures employed in the RFID systems. Its structure relies on a one-way hash function and it was first proposed by Weis in 2004. The hash lock scheme solves the privacy issue, but the tracking problem is not solved by this algorithm. A solution to this is the *Randomized Hash Lock* [2] algorithm, which solves the privacy and tracking issues of individuals. Both of these approaches still suffer from the problem of scalability: in both of the schemes, for communication between a tag and a reader to succeed, the reader must check all of the possible secret keys of the tag. In large scale systems, this is infeasible.

In [3], Ohkubo *et al.* proposed a scheme in which each time a tag is read, a hash function is applied to the identification number of the tag. Then by employing a second hash function, the identifier is hashed once again. Although their proposed scheme keeps the privacy of the users and also provides forward security, it poses a great computational load to the backend database system. This is because in this algorithm, all of the possible hashes must be calculated until a collision happens.

Unlike the previous scheme, a protocol designed by Henrici and Müller [4] adds the concept of a Transaction Number (TID). Once a request is received from the reader, the tag increases its transaction number by one and sends to the reader a hash of its ID, a hash combination of its current transaction number and its ID, and finally $\Delta\, TID$, which is the subtraction of existing transaction number from the number of the last successful transaction. The major weakness of this scheme is again the scalability problem. When the number of tags grows, the number of stored identifiers will also increase at an exponential rate.

The *YA-TRAP* communication protocol [5] was proposed by Tsudik in 2007. In this protocol, the tag, the reader, and the database server share a common secret which differs from other available secrets in the system. The YA-TRAP protocol will be started, once the reader sends the recent timestamp (T') to the tag. Then, the tag will check whether the recent timestamp is newer than the previous one (T) or not. Moreover, it checks to know if the recent timestamp is bigger than T_max. If these assumptions are not true, the tag only utilizes a pseudo-random number generator in order to produce k-bit random number. If not, it registers the latest timestamp and calculates its hash value (h) by using the secret key (x). Finally, the reader sends (H) (which was firstly sent from the tag to it) to the server for authentication purpose. In his protocol, Tsudik recognizes two important weaknesses. First, this protocol is vulnerable to a *Denial of Service Attack (DoS)* once an attacker disables the tag either permanently or temporarily or sends a wrong timestamp to the receiver side. The second vulnerability which is known as *Replay Attack* occurs when the timestamp is merely used for authentication purpose. In this attack, an attacker is able to send some sequences of expected timestamps to the tag and record its responses. Once the times in these timestamps become real, it can reply to all requests from the reader properly without the presence of the tag.

In addition to the presented weaknesses concerning the communication among tags and reader in RFID systems in general, another major problem in such systems is load of server to detect (identify) RFID tags. To solve this problem, *Tree-Based Private Authentication Scheme* was proposed by Molnar. [6] In his proposal, Molnar presented that, each tag will be identified with a leaf of the tree. Once a reader requires to be identified by a tag, the procedure will start from the root of the tree (there is no difference to start from either left or right). However, this scheme is vulnerable to the data leakage. It means that if an adversary can capture some of tags in the system, she might be able to have access to the secret keys from the root to the leaves. Thus, she can compromise the secret keys of non-captured tags.

As can be deducted from the presented security communication algorithm, each of them still suffer from some major problems showing that they are not secure enough in order to be proposed for safety-critical applications (i.e. RFID implant systems). Thus, to benefit from such protocols, they need to be optimized based on the necessary specifications of implantable systems.

2. Implantable Medical Devices

There are already several different implantable therapeutic devices in use in different healthcare solutions. Although a significant part of non-biodegradable implants such as artificial joints can function without considering ICT devices, other devices such as heart pacemakers have become notably complicated in recent years. They can integrate sensors of movement to adjust the heart rate, create logs from the biological data and communicate through radio frequencies with the external world. Such multifunctional and sophisticated devices are classified as Implantable Medical Devices (IMD). The functionality of these devices is not based on a periodically repeated routine. [1] However, some of the functions trigger automatically as a result of continuous monitoring of the patient's body by means of sensors embedded in the IMD. Therefore, such devices require two-way communication between them and the external world.

RFID implants — as a recent application of RFID systems — are introduced into the human body in order to facilitate identification and authentication processes of humans everywhere. In such system, the identification process can be done completely automatically and there is no need to type, confirm and remember passwords or even to carry a token. As opposed to for example iris scanning, RFID implanted users do not need to clean their hands or stand still for the identification process.

Commercial RFID implants being used for people are passive tags, meaning that they do not need any built-in battery and their operation relies on energy that is emitted by an external RFID reader. Because such tags do not have any moving parts, once implanted they can remain activated for more than 10 years. However, their notably small size and lack of internal power supply limit their performance in terms of processing power, communication range, and memory. The hardware limitations make the design of RFID implants that include advanced authentication procedures very complicated. ICT implantable devices (i.e., RFID implant systems) can be divided into two categories: *Static Systems* and *Dynamic Systems*. In static systems, the available information concerning the implanted device (for example, the medical history of a patient) can be updated or modified by authorized person(s). In a dynamic system, in addition to the basic implant system components there are also sensor(s) for gathering information from the environment. These additional features of dynamic implants naturally result in increased power consumption in comparison to static implants.

3. Implantable Device Application Requirements Analysis

Before we can approach the topic of security requirements for implantable devices, we must first define the context for applications in which such devices will be used. While there are several potential use cases and applications, we can divide them into three main categories: *identification* applications, *financial* applications and *medical* applications. Each of these categories provides us with differing contexts and sets of requirements, which are sometimes in conflict with requirements from other categories. All of these devices have one common requirement: as they are implanted to the human body, they must not cause any harmful side-effects to human physiology by their presence.

A. Identification Applications

Implanted RFID identification devices link a person and an identity to a certain implant ID, so when a particular ID is encountered we can ascertain the actual identity behind such an ID. For this to work, the system requires a back-end database where all ID-identity pairs are stored.

The application requirements for identification implants can be derived from other, more conventional methods of how we identify ourselves, such as picture ID cards. Just like an ID card, the implant must have a distinctive identifier or multiple identifiers that can be used to link the person to the identification device. ID cards use biometrics (typically a photograph and a fingerprint) as the identifier, and as such they are intuitive for people to use, as we are biologically accustomed to matching faces with identities. An implant has a unique ID corresponding to the implant bearer. Another important requirement is that it is very hard to copy or forge such an item that can be used for identification. ID cards have several countermeasures directed against forgery attacks, so implants must have at least equivalent resistance against forgeries.

B. Financial Applications

If an implant were to be used as a method of payment, the requirements for security are necessarily stricter, as financial matters are heavily regulated by governments. The use of implants as a method of payment is not new, but it has been done in the past [7]. The requirements for financial applications are effectively a superset of the requirements for identification applications, as the included financial dimension adds more restrictions to what can actually be done with the system. Linking an identity to an implant and then adding for example credit card details to this information presents the back-end system with stricter requirements for security, privacy and integrity of data.

C. Medical Applications

The majority of current implants fall into this application category. IMDs are used to augment the capabilities of the human body in cases of failure, or to monitor its behavior. Classical examples include artificial joints and pacemaker devices.

All computer-based medical devices must pass very strict evaluations before being allowed to be used in treatments. The incidents caused by the faulty Therac-25 device are a prime example on the problematic combination of computers and medical devices [8]. The possibility of an implant causing damage to or even death of the patient is significant if the implant actively interacts with the body. This makes patient safety the most important requirement for medical applications.

The data gathered and handled in medical applications is by its nature very private and confidential. Doctor-patient confidentiality regarding medical matters is taken very seriously in all and any jurisdictions in the world, so automated systems which also handle such data must provide very secure methods for handling, transmitting and storing such data.

D. Legal Ramifications for Implantable Devices

While legal questions are necessarily tied to individual countries and their legislation concerning implantable devices, we can nevertheless address certain universal juridical issues. In-depth discussion on legal dimensions of implants is beyond the scope of this paper.

The medical device modifications of 1976 provided primary authority to the U.S. FDA in order to control medical devices as well as to attain “reasonable assurance of efficiency and safety” before marketing [9]. Each type of medical device is allocated by the FDA into one of three regulatory classes based on their risks and needed evaluations to determine efficiency and safety of such devices [10][11]. Most of class I devices such as stethoscopes are low-risk and they are merely subjected to general regulatory control. Class II devices such as computerized tomographic scanners must fulfill requirements for general regulatory control as well as special regulatory control, for instance requirements for special labeling. Class III products such as deep brain stimulators and implantable cardioverter–defibrillators necessitate clinical studies to evaluate their safeness and effectiveness as medical devices for a Premarket Approval (PMA) application [12]. Class III devices which derive from alterations to previously PMA-approved devices may not require further clinical studies [13]. Furthermore, some older class III devices that the FDA has not definitely entitled for PMAs can obtain approval through the 510(k) section of the Food, Drug and Cosmetic Act [14].

Until the 1990s, each country had its own guidelines to evaluate medical devices [20]. To standardize an unequal and complicated market, E.U. directives outlined requirements by which each medical device could be marketed through all E.U. member states. This is possible

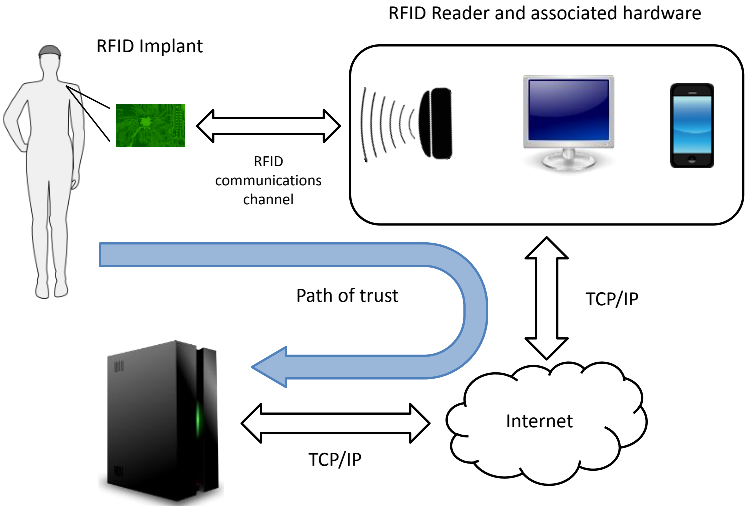
RFID Reader and associated hardware
RFID Implant
RFID communications channel
Path of trust
TCP/IP
Internet
TCP/IP

Figure 1 – Communication between RFID implant and back-end database

once a device earns a Conformité Européenne (CE) sign in any of member country [21][22]. These directives categorize medical devices into four different classes: I, IIa, IIb, and III. The categorization is based on risks caused by the expected usage of the devices [15]. In the European Union and the United States data requirements for medical devices can vary considerably. Nevertheless, such requirements must be prioritized so that they maintain a balance between the safety, the security and the privacy of the implanted patients. For instance, a device for left atrial appendage prohibition (for avoidance of brunt in atrial fibrillation) received a CE mark in 2009 based on pilot data whereas it was rejected by the FDA due to safety concerns, including technical difficulties and high amounts of stroke, appearing from a study on 700 patients conducted as part of a PMA [24][25][26].

4. Trust Issues in Implantable Medical Devices

As medical information is highly personal and clearly within the sphere of private confidential information, the utmost care must be taken that it will not fall into wrong hands. Doctor-patient confidentiality is usually codified in law in most countries, and violations of this trust are considered a serious offense. Therefore, when we examine RFID implants with associated medical information linked to them – even indirectly via a database – we must be able to trust the whole chain of devices which handle data, and the communication channels utilized for transmission of data.

A. Trust, Computation Platforms and Communications Channels

A communication model for RFID implants with a back-end database is demonstrated in Fig. 1. The implant communicates with a reader brought to physical proximity, and the reader then communicates with the back-end database system containing the actual sensitive information. The system must be constructed in such a manner that it is impossible to gain unauthorized access to any of these communication channels. The connection between the implant and the reader must be encrypted so that it cannot be eavesdropped upon. This requires that the implant and reader both support the same encryption algorithms and secure protocols. The communication between the reader and the back-end database is done over the Internet, and here we can use the existing infrastructure for secure communication. The connections should be encrypted, the common method being Transport Layer Security (TLS), and the certificates used in establishing these connections should be only from trusted sources. This may, for example, place additional requirements on the Certificate Authority (CA) providing the certificates.

We must also consider the computing platform to which the reader is connected to. If the reader is not a standalone device with its own internet connection and necessary features for accessing and displaying the data from the backend database, it must be connected to a PC, smartphone, or equivalent computer device. These components can also be compromised by attackers. In this case, all information that is processed on the PC will be also available to the attackers.

We must be able to trust the communication channels to be secure enough that no attacker can with reasonable resources breach them. The platforms which process the data must also be secure and auditable. In this paper we only consider the security of communication channels between the implant and the reader, but the other channels and platforms are equally important to secure. The path of trust depicted in Fig. 1 demonstrates the critical path upon which we must be able to trust all components processing data, and all communications channels used to transmit data.

In this paper, we assume that the methods for ensuring trust and secure communications over the Internet are adequate to the requirements of processing sensitive data. It can be argued, though, that due to the recent revelations on trunk network level wiretapping of the Internet by intelligence agencies [9] and potential compromises of master signing keys [28][29], these assumptions may not be true in the present situation. It remains to be seen whether the current infrastructure of the Internet is up to the challenges posed by these changes in the environment. Addressing these concerns, however, is beyond the scope of this paper.

5. Ethical Concerns

There are attempts at defining ethical rules and guidelines that are close to the field of RFID/ICT implants. In addition to the British Computer Society Code of Conduct [32] , the ACM Code of Ethics and Professional Conduct [34] has focused on several numbers of ethical studies. Such studies are, however, rather general as they are not specifically focused on either RFID tags or ICT implants. In 2007, the American Medical Association (AMA) officially established a code of ethics designed to protect implanted patients [35]. AMA's code of ethics is an accepted guideline for professional doctors or nurses. In reality, AMA's code of ethics is often used by both governments and courts as a guideline. To derive more precise requirements for RFID ICT implants from the ethical perspective, in the following we explore the topic of ethics a bit further.

Ethics is the philosophical study of morality. It can be described to be a rational examination into moral beliefs and behavior. Initially it may seem very hard for the ethical theories to keep up with the changes in modern society and information technology. At a closer look, however, it can be observed that humans tend to think and behave like the ones 2,400 years ago did, at the time when the Greek philosopher Socrates lived. The formal study of ethics goes back to his thoughts. When it comes to morality or ethics, arguments and counterarguments will never cease. Since the philosophy of Socrates (which was written by his student Plato), the philosophers have proposed many ethical theories. The problem is how to define a useful theory. It should allow its proponents to examine moral problems, reach conclusions, and defend them in front of skeptical arguers.

Relativism is the theory that there are no universal moral norms of right and wrong [36]. According to Relativism, if one is willing to receive an RFID implant, it is right for that one but not necessarily for others. A different view can be obtained from Kantianism. According to Kant’s second formulation of the categorical imperative, one should “Act so that you always treat both yourself and other people as ends in themselves, and never only as a means to an end”. Considering RFID implants, they should be beneficial to the implanted person, not for others for example for gathering information. The Principle of Utility is a clear contrast to Kantianism: “An action is right (or wrong) to the extent that it increases (or decreases) the total happiness of the affected parties” [36]. Considering RFID implants, the happiness could be interpreted to indicate increased security; not an easy calculation.

Bioethics is a branch of applied ethics which studies moral values in the medical science and biology. It is commonly referred to the morality of medical and biological procedures, like the use of stem cells harvested from aborted embryos, abortion itself, different life-supporting measures, assisted suicide and so on. The definition is very difficult and the boundaries obscure. RFID implants might be considered as falling into the category of bioethical problems. If medical research, life support, human enhancement, body modification and so on involve bioethical concerns, then clearly the ethics of RFID implants should also be considered as bioethical concerns.

There is a vast amount of different active and passive devices implantable into a human body for example for the purposes mentioned above. Most of these devices are implanted for life-saving or life-maintaining purposes, and some to improve the quality of life. An RFID implant can be a life-saving instrument if it contains critically important, otherwise unobtainable information for example in a trauma case involving an unknown, unconscious person.

The technology has to be securely developed, so that it in no case could interfere with other devices implanted, connected, or otherwise used or in contact with a person. The implant cannot have any influence under no circumstances with life-supporting devices for example in a hospital environment. All possible IMD:s have to be considered: pacemakers, stimulators, shunts, valves, stents, implantable drug pumps, cochlear implants and so on [37]. If the RFID implant cannot be inactivated, for example if it would somehow interfere with other IMD:s, it has to be surgically removed. The device has probably grown into the body: the body treats the implant and the surrounding area as “injured” and a “foreign body”; thus the body forms an excess amount of fibrous tissue (collagen) to repair the damage. The implant is small, but there are actually quite a lot of people who are prone to forming too much scar tissue around the device (or any other “injuries”). The result could be a hard lump many times bigger than the device inside it. This might for example impair hand movement and be painful.

Ethics is always a complicated issue, but it gets even more so when dealing with people with impaired cognitive capacities. The Decision-Making capacity has to be determined. This includes finding out whether the patient is capable legally, psychologically or otherwise to make adequate decisions including receiving implants. This is the question of the autonomy of the patient. Actually this question is more complex than the standard ethical models, which tend to be limited to considerations of the patient’s autonomy and beneficence. [38]

When considering the possible risks and outcomes of implanted RFID-tags, we have to consider the added value: whether there are some other not that risky ways to have same benefits. Considerations:

A) Awareness

1) The person who makes the decision has to be aware of all facts concerning the implant. It has to be ensured that he understands all the possible physical, medical and possibly the psychiatric consequences individually for him: for example

the formation of keloid tissue. The implant should be easily detectable because it affects various medical procedures; MRI scanning for example. Removability and usability need to be considered, implant location is a key factor here.

2) The individual should be aware of any information the implant contains, how critical the information is and what possible uses does this data have. The individual has to be made aware of all possible benevolent and malicious uses.
3) The implanted person has to know when the data is read, by whom and which data is actually read: privacy and security.
4) The authenticity of the data; if something is added, altered or updated, the person has to know. System-wise this means that an activities history (I/O log) needs to be maintained.

B) Pros vs. Cons (Added value)

1) The system should provide significant benefits in comparison to potential risks. Risks should be minimalized.
2) The system should be context-aware, so it actively thrives to recognize and minimize the threats and especially the consequences thereof. A great challenge here is that this should not increase the complexity of the system. It should not increase the need for communication between the system and the environment. This might mean that the practical computational capacity and power budget is exceeded.
3) The implant should be individualized so that the person could by himself tailor the implant just for his needs. The western society today is highly individualized; the pros and cons are subjective. The format would be standardized, but the information content of the implant could be individualized by the user.

C) Contextual data

1) Religion, beliefs, race, sexual orientation, political opinions and all such data should be considered because this kind of data may have tremendous impacts in special situations. For some people religion is the dominant factor in their lives, and all things are considered in the context of this religion; so this can be vital information. On the other hand people can be persecuted because of their religion; this is a dilemma. This kind of data should be available only on special situations.
2) The information of an emergency contact person should also be included. The word "spouse" should not be used to avoid discrimination or prejudice for example because of sexual orientation. If the data could be eraseable by the person himself, or it were possible to deny access to selected data, the person himself would implement context-awareness.

Careful consideration of these concerns has to be done both in designing RFID IMDs and in making a decision to actually implant a person with such a device. We see that most of these concerns can be resolved by developing novel technologies for RFID IMDs.

6. Security and Privacy Requirements Analysis

A framework for evaluating different security and privacy requirements for implantable medical devices is presented in [39]. These requirements are divided between security & privacy and safety & utility. This framework is meant for broad scope observation of implantable medical devices, ranging from simple passive implant tags to complicated active devices. We will use it as a basis for our analysis, and to derive key security requirements and make observations on their order of precedence, as some requirements can be in conflict with others.

A. Safety & Utility Requirements

Safety and utility goals encompass requirements for the safe and useful operation of IMDs [39].

Data access – the data stored, processed and transmitted by the IMD must be available to medical personnel upon request. This must be true in emergence situations as well.

Data accuracy – the data collected by the device must be accurate, and must also contain a timestamp.

Device identification – the device should identify itself upon request by authorized parties. The presence and nature of an IMD is important information when a patient is receiving treatment.

Configurability – the settings of the device should be modifiable by authorized parties upon request. Also, some devices must be able to be controlled by the person with the implant.

Updatable software – the firmware of the device, and other parts of its software must be upgradable by authorized parties.

Multidevice coordination – if there are several IMDs present, they must be able to communicate between themselves. Sharing data of different measurements of physiological events can be used to improve performance of devices. At the minimum, the devices should not interfere with each other in any manner.

Auditable – the device and its functional history should be auditable in the case of system failure.

Resource efficient – the device should use as little energy as possible to provide maximal lifetime for the IMD.

B. Security & Privacy Requirements

Security and privacy goals encompass topics related to data privacy and security [39].

Authorization – only authorized parties should be able to access the device, its functions and data. In emergency situations, the device should balance harm to the patient with harm form unauthorized access to the device.

Availability – the device should be resilient to Denial of Service (DoS) attacks, and a malicious entity should not be able to affect the operational capabilities of the device in any way.

Device software and setting robustness – it should not be possible for an attacker – whether an outsider, the patient, or the physician – to be able to modify the software or to trigger a specific operation of the device, or to modify other access control rights.

Device-existence privacy – the presence of an IMD should be hidden form unauthorized parties.

Device-type privacy – the exact type and functionality of the device should be hidden from unauthorized parties in the event that its existence must be revealed.

Specific-device ID privacy – the device should protect itself from tracking attacks based on its ID to protect location security of the patient.

Measurement and log privacy – only authorized persons should be able to access log and measurement data.

Bearer privacy – the bearer of a device should not be identifiable based on the IMDs properties.

Data Integrity – the data collected and stored by a device must be protected from tampering by unauthorized parties.

C. *Threat Scenarios*

There are wide discussions concerning the privacy and security issues of RFID implant systems. On one hand, security professionals are warning explicitly about the risks caused by such technology. On the other hand, implanted users are always concerned about the risks to their privacy. People are more vulnerable to privacy attacks since implantable tags can be linked to their body either temporarily or permanently. Although any other information conveyed by a tag is secured by cryptographic schemes, there is a risk that the location or position of an implanted user to be tracked via the implant itself. One of the major reasons that an implantable tag causes privacy concerns is that general purpose RFID tags usually respond to any queries they receive. Since humans are unable to sense the frequencies or communications transmitted among tags and readers, it causes tags to become a good target for eavesdropping.

Furthermore, when personal information of implanted users is linked to the RFID tag, not only they may be tracked by an adversary, but also users may be subjected to further privacy violations. For instance, in an RFID implant system, if an adversary is successful in impersonating a trusted component of the system (e.g. a reader), he can access personal information of the implanted user and exploit it for malicious purposes. The information can be related to the user’s medical history, social security number, bank account or other critical information. Likewise, in authentication applications, there is a risk of physical damage to implanted users. The major reason is that an adversary may want to extract the implanted tag from the user’s body by force. This is similar to the risk generated by using biometrics as an authentication method, as there are known cases where bodily harm has resulted from extracting an identifier from a person [40].

As the above discussion and security requirements attest, there are three main types of privacy concerns which are caused by RFID implant technology: location privacy, information privacy and decision privacy. Some of the most prevalent attacks concerning the RFID implant systems are presented as follows [41]:

Eavesdropping Attack: This attack is one of the most significant threats against RFID implant systems. Such attacks are generally dangerous because they can be done at a distance and are difficult to detect, as they are entirely passive. In the eavesdropping attack if an adversary can capture the traffic between the tags and the readers, she can access the transferred information if there are no other countermeasures in place.

Replay Attack: all messages transmitted between a tag and a reader can be captured and saved by an adversary. Then, it is possible for that adversary to impersonate either a tag or a reader in an RFID implant system. The most famous example regarding such an attack is to gain access to a restricted area. This can be done by replaying the captured traffic to a reader.

Jamming Attack: Such attack is done by broadcasting any kind of radio signals that can interfere with the communications of an RFID system by reducing the available signal to noise ratio. Thus, the availability and integrity of a communication can be attacked by disconnecting the air interface between the tag and the reader. This is a special Denial of Service (DoS) attack against a wireless system.

Man-in-the-middle attack: in an RFID system a man-in-the-middle attack is a kind of attack where an attacker manipulates the messages between a tag and a reader. This can be done by inserting, denying, or relaying the messages. This type of attack is against the integrity of communications.

Tracking of the Tag: a tracking attack is directed against the privacy of the tag holder. For example, the behavior of a person who is implanted with an RFID tag can be tracked by any unauthorized person. This can be done once an adversary pretends himself/herself as a trusted reader in the RFID implant system. By doing so, when the RFID tag and the RFID reader start to communicate to each other, the adversary will be enabled to track the implanted person illegally and access to his/her confidential information. Consequently, there is a risk that the information gained from the implanted person could be utilized in malicious ways in future.

Denial of Service Attack: It means to means to deactivate the RFID implant systems either entirely or partially (e.g. by disrupting the tag or the reader).An adversary may also disrupt the backend database either permanently or temporarily. Thus, the database system may be damaged so seriously that it may need to be replaced or reinstalled.

7. Hardware Requirements Analysis

The scale of possible hardware solutions differs significantly based on the target application. We must consider simple RFID tags separately form more complex IMDs. Principally, RFID tags are divided into high-cost and low-cost tags. High-cost tags are further classified as simple and full-fledged. Simple tags support one-way hash functions and random number generators, while full-fledged tags support public key functions, cryptographic one-way functions and symmetric encryption algorithms. Similarly, low-cost RFID tags are divided into *lightweight* and *ultra-lightweight* tags. Lightweight tags support CRC checksum calculation and random number generators, but ultra-lightweight tags can merely compute simple bitwise functions such as AND, XOR and OR. [42] This makes it practically impossible to implement standard issue cryptographic algorithms. More complex IMDs have their own power source and can accommodate more processing capacity if necessary for the application. Here we will focus on high-cost RFID tags, as they have the capability for complex cryptography operations necessary for implementing advanced security schemes.

Hardware footprint and power consumption limitations and security level requirements of RFID implant systems differ from mainstream applications of RFID due to the safety-critical specifications and delicate use cases. In comparison to RFID systems in general, which due to their nature of functionality require more logic elements to be implemented and consume much power, the area overhead and power consumption of RFID implant systems must be optimized.

Implantable tags are very small in terms of size and computational capacity. They also typically lack an internal power source, unlike full-fledged IMDs. Thus communication solutions for implantable tags must be relatively lightweight.

The major disadvantage of public key cryptography schemes based on integer rings ($\mathbb{Z}_p$) is that they have to use key sizes of 2048 bits or more to provide sufficient security [43]. This will increase the number of computations which in turn increases power consumption. The most widely known example of such a cryptosystem is RSA [44].

In the case of larger IMDs, we can assume them to have their own power source designed to last for significant amount of time, up to several years. This gives the possibility of using more robust protocols for increased security. The protocol suite and associated ciphers must still be carefully selected to minimize power draw from the internal battery, because IMD power sources are hard to replace and such operations present significant medical risks. One solution for extending the lifetime of implants and providing enough power for more energy-intensive cryptography applications is to use batteries that can be charged wirelessly through magnetic induction [45]. This extends the life of an IMD significantly and alleviates the requirements for power consumption optimization.

8. Secure Communication Protocol for RFID Implant Systems

A secure and lightweight communication protocol for RFID implant systems with the necessary cryptography algorithm support is sketched in this section. The protocol consists of four different phases.

1. The reader authentication phase

This phase can be done based on Okamoto's witness hiding identification algorithm [50]. Previously, in [47] Martinez et al. proposed Schnorr's zero knowledge proof using elliptic curve cryptography to authenticate readers in RFID systems. Schnorr's identification protocol is efficient. However, the major concern of Schnorr's protocol is that it is proved to be zero-knowledge just for an honest verifier and it is not trustable since there might be cheating verifiers in the system. By using n repetitions of Schnorr's protocol, the complexity of the protocol will increase by a factor of n. Thus, we propose to employ Okamoto's witness hiding identification algorithm to authenticate readers in RFID implant systems efficiently. Fig. 2 presents a reader authentication scheme based on Okamoto's witness hiding identification algorithm.

In this algorithm, assume that G is a group of order n, where n is a large prime number and $g_1, g_2 \in G$ are selected randomly in G so that $log_{g_1}\ g_2$ is unknown to anyone. Moreover, suppose that $y_1, y_2 \in \mathbb{Z}_n$ are the private key of the prover, and on the other hand, $k = {g_1}^{y_1}{g_2}^{y_2}$ are the public key of the prover. In Okamoto's algorithm, it is shown that, for the generators g_1, g_2 and also a particular public key k, there are exactly n possible pairs $(y_1, y_2) \in Z_n \times Z_n$ which satisfy the equation $k = {g_1}^{y_1}{g_2}^{y_2}$. If y_1 is fixed as $y_1 \in Z_n$ then y_2 can be defined as $y_2 = log_2^{(k/g_1^{y_1})}$. The pair (y_1, y_2) is known as 'witness'. In our approach, the private key of the RFID reader is defined as a witness (y_1, y_2).

Tag		Reader
$k = {g_1}^{y_1}{g_2}^{y_2}$		
$x_1, x_2 \quad \in \mathbb{Z}_n$		
$a \leftarrow {g_1}^{x_1}{g_2}^{x_2}$		
	$\xrightarrow{a}$	
		$d \in \mathbb{Z}_n$
	$\xleftarrow{d}$	
$w_1 \leftarrow x_1 + dy_1$		
$w_2 \leftarrow x_2 + dy_2$		
	$\xrightarrow{w_1, w_2}$	
		${g_1}^{w_1}{g_2}^{w_2} \overset{?}{=} ak^d$

Figure 2 - Reader authentication scheme

2. *Tag Identification Phase*

The tag identification phases which rely on Elliptic Curve Cryptography (ECC) [46] are done once an RFID reader (which has been successfully authenticated) tries to read a tag in the system. In this phase, every tag holds a secret $K\langle i,j\rangle$, which belongs to elliptic curve $E\ (\mathbb{F}_g)$, and it varies in each reading operation. The main reason is to avoid reading the same tag in a way that could be correlated by an adversary. Whenever a tag is read, its current ID ($ID\langle i,j\rangle$) is sent to the reader (i corresponds to the tag and j is the number of reading). The tag's identification phase is done in three steps below [47]:

a. The tag calculates its ID in such a way that $ID\langle i,j\rangle = Lib\left(x\ (K\langle i,j\rangle)\right) * Lib\left(z\ (K\langle i,j-1\rangle)\right)$ where $x\ (K\langle i,j\rangle)$ and $z\ (K\langle i,j-1\rangle)$ are the abscissa and the coordinates of the existing and previous secret points, and Lib presents some last bits of the input bits, and finally '$*$' is a none-algebraic operation over $\mathbb{F}_g$. This operation can be either a bitwise xor (if the field is prime) or a modular addition (if the field is binary).
b. Then, the next secret point of the tag will be calculated as $K\langle i,j+1\rangle = aG$, where a is the product of a specific function f to the abscissa of $K\langle i,j\rangle$ and it is written as $a = f\ (x\ (K\langle i,j\rangle))$.
c. Finally, the tag keeps its new secret point and its ID will be sent to the reader.

3. *Tag Verification Phase*

By this time, the reader has received the $ID\langle i,j\rangle$. Therefore, it is required to access the database in order to verify the tag's identity. To have an efficient identification, the database server must keep the outputs for all available tags $ID\langle i,j\rangle,\ i \in [1,n]$ (where n is the number of tags) in the system. Moreover, the database server should keep the corresponding secret points $k\langle i,j\rangle$ accessible. These values are kept in a hash table to be accessed easily on request. Once a trusted reader gets an ID, it is sent to the backend database. The backend database searches for it in the hash table, modifies the corresponding secret point at the same time, removes the previous $ID\langle i,j\rangle$ from the hash table, and inserts the new one. As the final point, all the required information will be received by the reader. [47]

In the larger environments where it may be possible that readers do not receive the ID (due to the noise caused by the attacker) of the tag, the tags may have updated its value without the corresponding update of the database. To avoid this problem, the tag needs to wait for an *Acknowledgement* (*Ack*) message (which comes from the reader's side) before storing its new secret value. The value of the acknowledgment message is computed by the database system and once it is calculated the message will be sent to the reader. The acknowledgment message may also be vulnerable to not to arrive. This is a less serious problem, the only result of this problem is that in the next reading of a tag, its old ID will be returned.

4. *Communication among Tags and Readers*

Once the RFID tag and the RFID reader are identified and authenticated as honest components of an RFID implant system, they start to transmit essential information or messages that are required to be conveyed. To provide secure and lightweight communications between tags and readers, we propose a new protocol based on Elliptic Curve Digital Signature Algorithm (ECDSA) [46] using the Quark lightweight hash function [48]. In our proposed communication scheme, first of all, an RFID tag needs to calculate the hash value (h) of the message m such that $h = HASH\ (message\ m)$. In this phase, the algorithm of $HASH\ (message\ m)$ is computed by considering the message m as the input value of the Quark lightweight hash design. Quark is one of the most recent lightweight hash designs. It was first proposed by Aumasson et al. in 2012. The design of Quark lightweight hash relies on non-linear Boolean functions and bit shift registers. Therefore, not only its implementation becomes feasible, but also, the circuit area requirements of this hash design are well suited for implantable medical devices.

Once the hash value is determined and before the result is sent to the reader, we propose that the result of the concatenation of the message m and its hash value h is encrypted using an efficient encryption algorithm.

$$H = enc\ (\ m \ \ \| \ h\ (m)\ ) \tag{1}$$

Once the encryption process of the concatenation of message m and its hash value h is completed, a random integer k , $k \in [1, n-1]$, which is the secret key, will be chosen by the tag. Then, with respect to the generator of the elliptic curve G having the order of n , the curve point (x,y) of the ECDSA algorithm will be defined as:

$$(x,y) = p = k * G \tag{2}$$

In the next step, the RFID tag calculates the values d, c and presents the pair (d,c) as its own signature:

$$d\ =\ x\ (mod\ n) \tag{3}$$

$$c\ =\ k^{-1}\ (HASH\ (m)\ +\ d * P)\quad (mod\ n) \tag{4}$$

Finally, the pair (d,c) will be sent to the RFID reader as the tag's valid signature. Once the reader receives the signed message from the RFID tag, it needs to have a copy of the tag's public key Q to authenticate the tag's signature. The reader is able to authenticate Q based on the following steps:

1. The reader computes whether Q is equal to the neutral element $\mathcal{O}$.
2. The reader computes whether Q exists on the curve.
3. The reader computes whether $n\ *\ Q$ is equal the neutral element $\mathcal{O}$.

Subsequently, to verify the signed message of a tag, the reader needs to do the following steps:

First, the reader needs to check whether the integers d and c are between the interval $[1, n - 1]$. Then, to get the message m and its hash value h, the reader needs to decrypt H (which is the encrypted expression of the concatenation of the message and its hash value) so that $W = dec\ (H)$. Once the message m and its hash value h are recognized by the decryption algorithm, to verify the signed message of the tag, the reader needs to compute the following equations. Note that r is the n leftmost bits of m.

$$T = c^{-1}\ (mod\ n) \tag{5}$$

$$V_1 = r.T\ (mod\ n)\ ,\ \ V_2 = d.T\ (mod\ n) \tag{6}$$

The Curve point (x, y) is calculated as:

$$(x, y) = V_1 * G + V_2.Q \tag{7}$$

Finally, the reader accepts the signature as a trusted one if:

$$d = x\ (mod\ n) \tag{8}$$

As seen in the previous discussion, our proposed communication security protocol for RFID implant systems employs robust and secure algorithms for identifying and authenticating tags and readers. The probability to have an unauthorized tag or reader in the whole system is 1/n (which is almost zero). From this point of view, there is no need for re-authentication and re-identification for communication between tags and readers. If for any reason an unauthorized tag or an unauthorized reader is recognized in the system, it will be declined prior to the time that the authorized tag and the authorized reader start to communicate to each other. As the communication and processing are required to be lightweight in an RFID IMD system, the additional computations imposed by re-authentication and re-identification would have a negative effect on the efficiency of the system, making it potentially infeasible.

9.Security Analysis

The security requirements of lightweight security schemes are almost similar to the conventional schemes which have been broadly discussed in cryptography literature. In this section, five prominent types of attacks against the security of our proposed protocol are studied and analyzed.

Tracking of the Tag— tracking the tag owner's behavior. For example, the behavior of a person who is implanted with an RFID tag can be tracked by any unauthorized person. This could be possible if an adversary pretends to be a trusted reader in the RFID implant system. By doing so when the RFID tag and the RFID reader start to communicate with each other, the adversary will have the ability to track the implanted person and access his/her confidential information.

In our proposed protocol, the only public information concerning the tag is its ID that is randomly generated and the current ID always differs from the previous one. At a specific time, any ID that is sniffed by an adversary cannot be associated with the information obtained after or before that time as the transferred data is generated based on the tag's secret key which is altered at every reading procedure.

Eavesdropping Attack— in an RFID implant system, with an eavesdropping attack the adversary can capture the communications conveyed between the tag and the reader. In this type of attack the adversary does not need to communicate with the RFID tag. He/she only captures the transmitted signals using RF equipment. As it was discussed earlier, the information gained by the adversary can be utilized later against the privacy of the implanted users. However, the successfulness of the adversary depends on the resources available for the attack.

On the one hand, in our proposed protocol we presented that, if an adversary can guess the tag's secret key $k\langle i,j\rangle$, the only public information being available concerning the tag is its ID. Previously in the tag identification phase, it was shown that the value of the ID results from the product of a non-algebraic operation that is done on the last bits of the abscissa and the coordinates of the two secret points ($ID\langle i,j\rangle = Lib\left(x\left(K\langle i,j\rangle\right)\right) * Lib\left(z\left(K\langle i,j-1\rangle\right)\right)$). Thus, it is impossible to compute and obtain the tag's secret key from its ID. The reason is that obtaining the secret points implies the computation of the elliptic curve discrete logarithm problem. Since solving the discrete logarithm problem is as hard as the integer factorization problem, it is not easily feasible to solve this problem. Thus far, there has not been any polynomial time algorithm proposed to solve discrete logarithm problems.

On the other hand, in the reader authentication phase we showed that in the communication between the RFID tag and the RFID reader, if a cheating reader can obtain the witness $\left(y'_1, y'_2\right)$, with the probability equal to $1/n$, the witness (y'_1, y'_2) gained by the cheating reader is identical to the reader's witness (y_1, y_2). Thus, with the probability of almost $'1'$, the two mentioned witnesses are unequal to each other.

Spoofing Attack— means to impersonate as the tag or the reader in an RFID implant system. Consequently, we need to consider two different spoofing attacks:

- *Spoofing of a Reader*: when there is no reader authentication protocol for secured communication in RFID implant systems, the adversary may be able to impersonate the reader. In our proposed protocol's reader authentication phase we showed that with the probability of $1/n$ the witness $\left(y'_1, y'_2\right)$ can be identical to the reader's witness (y_1, y_2), but we also presented that the tag accepts the reader as a valid one only if the verification $g_1{}^{w_1} g_2{}^{w_2} = ak^d$ holds.

- *Spoofing of a Tag*: In the tag spoofing attack, to impersonate a tag, an adversary needs to have an access to the tag's current secret $k\langle i,j\rangle$ and this value cannot be acquired from the public information of the system. However, in a case that an adversary learns the tag's secret physically, returns the tag back to the system (without modifying it) and impersonates the tag just before a trusted RFID reader reads it, then the actual tag's secret will be obsoleted since the expected ID of the tag will be modified by the backend database system. Thus, the tag may become a target of a denial of service attack.

Denial of Service Attack— to deactivate the entire RFID system or part of it temporarily or permanently. In our proposed protocol in every reading procedure (after having a successful reader authentication) the RFID tag modifies its current secret $k\ \langle i, j\rangle$, so there is no risk that an adversary does a denial of service attack to the tag. However, the backend database system can be affected by the *DoS* attack since the generation of the tag ID is done over the database system. An adversary may disrupt the backend database permanently or temporarily. Thus, the database system may be damaged so seriously that it may need to be replaced or reinstalled. To avoid the database being disrupted, having an acknowledgement message can be considered as a solution. Note that the choice of acknowledgment message may depend on the environment in which the RFID implant system is utilized. It means that the value of this message may vary from one environment to the other one.

Replay Attack— means an attacker resends the information which it had captured and eavesdropped in previous sessions. In our proposed scheme, we showed that with the probability of $1/n$ the adversary's witness (y'_1, y'_2) can be identical to the reader's witness $(y_1, y_2\ )$. Furthermore, an attacker is not able to reuse the tag's ID, since the database server always waits for the next ID of each tag and the tag's ID will be updated once a new one is inserted. Therefore, if an adversary tries to reuse a tag's ID, it will inhibit the reader to identify the fake ID as a correct one.

As it was presented earlier, for the communication between tags and readers in an RFID implant system, we gain benefits from using the D-Quark lightweight hash function instead of utilizing general purpose hash designs like SHA-1 or SHA-3. To proof our claim, we will compare the complexity of collision and pre-image resistance of D-Quark lightweight hash function and other general purpose hash designs.

SHA-1 has been proposed several times in literature to be employed in security algorithms of RFID systems. However, since February 2005, there have been several successful attacks announced by cryptanalysts regarding the SHA-1 hash design. Consequently, they suggest that SHA-1 algorithm is not secure enough to be used for current delicate technologies. As a result, a new family of SHA known as SHA-2 was developed. Although no efficient attacks have been announced against the SHA-2, its algorithm is still similar to SHA-1. In 2012, another family of SHA hash design known as SHA-3 (Keccak) was proposed. However, since the major focus of the SHA-3 is on its software performance, it is not efficient to utilize SHA-3 for guaranteeing the security of RFID systems [48]. Table I presents complexity computation results concerning the collision and pre-image resistance of D-Quark, SHA-1 and SHA-3 having 160-bits digest.

TABLE I. SECURITY COMPARISON OF D-QUARK LIGHTWEIGHT HASH FUNCTION WITH OTHER HASH DESIGNS (BIT) [48]

Hash Function	Digest (bit)	Collision	Pre-image Resistance
SHA-1	160	2^{61}	2^{160}
D-Quark	160	2^{80}	2^{160}
Keccak (SHA-3)	160	2^{80}	2^{160}

10. CONCLUSION

In this paper, we derived an engineering specification for functionality, security, and implementation demands for RFID Implantable Medical Devices (IMD) requiring medical data storage and wireless communication. Due to the high capacity computations needed by conventional cryptography algorithms, communication security solutions proposed based on such algorithms are not efficient and not necessarily even feasible to be employed for RFID implant systems. Therefore, lightweight cryptographic algorithms have been proposed for the application. As implantable tags are mostly passive, their small size and lack of internal power source limit their performance in terms of processing power, communication range, and memory. The hardware limitations make the design of RFID implant systems extremely complicated.

Our specification follows from a requirements analysis of application characteristics, legal restrictions, security requirements and ethical concerns of IMDs. We identified the key ethical issues relating to RFID technical specifications as the following: 1) Awareness; The Autonomy of a person has to be guaranteed, on the other hand the matter of beneficence has to be taken into account, 2) Added value; Benefits for the individual person outweigh the risks and 3) Contextuality; The tag has to be adabtable by the person himself or his surrogate/custodian according to different situations.

In addition to some particular areas where RFID systems have been employed including asset tracking, animal identification, entrance access control and so on, nowadays humans are also approaching to the fore. Implantable tags can be introduced into the human's body to simplify authentication and identification of them everywhere. Based on the results we acquired by optimizing the communication security of RFID implant systems using lightweight cryptographic algorithms, not only our proposed protocol is secure and robust against different types of well-known attacks, but also, our proposed protocol consumes less power and requires less hardware footprint to be implemented.

Our specification considers the special operating environment, delicate use cases and safety-critical functionality of IMD systems and it is aimed to become a conceptual platform for designing robust security schemes and long-term functional and physical reliability.

REFERENCES

[1] M. N. Gasson, E. Kosta and D. M. Bowman, *Human ICT Implants: Technical, Legal and Ethical*; Netherlands: Springer-Verlag, 2012, pp. 11-158.

[2] S. A. Weis, S. E. Sarma, R. L. Rivest, D. W. Engels, *Security in pervasive Computing*; Germany: Springer-Verlag, 2004, pp. 201–212.

[3] M. Ohkubo, K. Suzuki, S. Kinoshita, "Cryptographic Approach to Privacy-Friendly Tags," Presented at the RFID Privacy Workshop, Nippon Telegraph and Telephone Corporation, MIT, November 15, 2003.

[4] D. Henrici, P. Müller, "Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers," in *Proc. 2th Annu. Conf. Pervasive Computing and Communications*, Washington, DC, 2004, pp. 149-153.

[5] G. Tsudik, "A Family of Dunces: Trivial RFID Identification and Authentication Protocols," *in Proc. 7th PET Conf.,* 2007, pp. 45-61.

[6] D. Molnar, D. Wagner, "Privacy and security in library RFID: Issues, practices, and architectures," in *Proc. 11th CCS Conf.,* 2004, pp. 210-219.

[7] P. Rotter, B. Daskala, R. Compañó, B. Anrig, C. Fuhrer. Potential Application Areas for RFID Implants. *Human ICT Implants: Technical, Legal and Ethical Considerations*; Netherland: TMC Asser Press, pp. 29-39, 2012.

[8] N. G. Leveson, C. S. Turner, "An investigation of the Therac-25 accidents," *Computer,* vol.26, no.7, pp.18-41, July 1993.

[9] Medical Device Amendments. Public Law 94-295 94th Congress. (May 1976). [Online]. Available: http://www.gpo.gov/fdsys/pkg/STATUTE90/pdf/STATUTE-90-Pg539.pdf.

[10] W. H. Maisel "Medical device regulation: an introduction for the practicing physician," *Annals of Internal Medicine*, vol. 140, no. 4, pp. 296-302, Feb. 2004.

[11] U.S. Food and Drug Administration. Medical devices: device classification. (April 2009). [Online]. Available: http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/default.htm.

[12] W. Sapirstein , S. Alpert , T. Callahan , "The role of clinical trials in the Food and Drug Administration approval process for cardiovascular devices," *Annals of* Internal Medicine, vol. 89, no. 4, pp. 1900-1902, Feb. 2004.

[13] United States Government Accountability Office. Report to Congressional Addressees: Medical Devices. (January 2009). [Online]. Available: http://www.gao.gov/assets/290/284882.pdf.

[14] D. B. Kramer, S. Xu, A. S. Kesselheim, "Regulation of Medical Devices in the United States and European Union," *The New England Journal of Medicine*, vol. 366, no. 9, pp. 848-855, Mar. 2012.

[15] European Commission DG Enterprise Directorate B. Unit B2. Medical Devices: Guidance document - Classification of medical devices. (June 2010). [Online]. Available: http://ec.europa.eu/health/medicaldevices/files/meddev/2_4_1_rev_9_classification_en.pdf.

[16] U.S. Food and Drug Administration. List of Medical Devices by Product Code. (November 2012). [Online]. Available:http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/UCM328694.pdf.

[17] British Computer Society Code of Conduct. Code of Conduct for BSC Members. (June 2011). [Online]. Available: http:// www.bcs.org/upload/pdf/conduct.pdf.

[18] Association for Computer Machinery. ACM Code of Ethics and Professional Conduct. (October1992). [Online]. Available: http://www.acm.org/constitution/code.html.

[19] B. Bacheldor. AMA Issues Ethics Code for RFID Chip Implants. (July 2007). RFID Journal. [Online]. Available: http://www.rfidjournal.com/article/view/3487/2.

[20] A. G. Fraser, J. C. Daubert, F. Werf, M. Estes, S. C. Smitt, M. W. Krucoff, P. E. Vardas, M. Komajda, "Clinical evaluation of cardiovascular devices: principles, problems, and proposals for European regulatory reform," European Heart Journal, vol. 32, pp. 1673–1686, May 2011.

[21] European Council Directive 93/42/EEC. Concerning Medical Devices. (June 1993), [Online]. Available: http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0042:20071011:en:PDF.

[22] European Commission. Classification of medical devices (MEDDEV 2.4/1 Rev. 9). (June 2010). [Online]. Available: http://ec.europa.eu/consumers/sectors/medicaldevices/files/meddev/2_4_1_rev_9_classification_en.pdf.

[23] Idem. Classification criteria: Annex IX of Directive 93/42/EEC. (June 2010) [Online]. Available: http://www.lne-gmed.com/pdf/en/ annex9-directive-93-42-amended.pdf.

[24] D. Holmes, V. Reddy, Z. Turi, S. Doshi, H. Sievert, M. Buchbinder, C. Mullin, P. Sick, "Percutaneous closure of the left atrial appendage versus warfarin therapy for prevention of stroke in patients with atrial fibrillation: a randomized non-inferiority trial," *Lancet Medical Journal*, vol. 374, pp. 534-42, Aug 2009.

[25] E. Cingolani, S. Stevens, M. Shehata, G. Diamond, S. Kaul, "Medical device regulatory reform: insights from the Watchman left atrial appendage closure technology for stroke prophylaxis in atrial fibrillation," Archive of International Medice, vol. 171, pp. 1670-1672, Oct 2011.

[26] W. Maisel, "Left Atrial Appendage Occlusion — Closure or Just the Beginning?" *New England Journal of Medicine* vol. 360, no. 25, pp. 2601-2603, June 2009.

[27] G. Greenwald, E. MacAskill, (June 2013). NSA Prism program taps in to user data of Apple, Google and others. The Guardian. [Online]. Available: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[28] J. Ball, J. Borger, G. Greenwald. Revealed: how US and UK spy agencies defeat internet privacy and security. The Guardian. (September 2013). [Online]. Available: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[29] N. Perlroth, J. Larson, S. Shane, N.S.A. Able to Foil Basic Safeguards of Privacy on Web. The New York Times. (September 2013). [Online]. Available: http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html

[30] M. Stephen, M. R. Dibben. "Trust, untrust, distrust and mistrust–an exploration of the dark (er) side." *Trust Management*. Springer Berlin Heidelberg, pp. 17-33, 2005.

[31] D. A. MacKenzie. *Inventing accuracy: a historical sociology of nuclear missile guidance*. MIT Press, 1990.

[32] European Commission DG Enterprise Directorate B. Unit B2. Medical Devices: Guidance document - Classification of medical devices. (June 2010). [Online]. Available: http://ec.europa.eu/health/medicaldevices/files/meddev/2_4_1_rev_9_classification_en.pdf.

[33] British Computer Society Code of Conduct. Code of Conduct for BSC Members. (June 2011). [Online]. Available: http:// www.bcs.org/upload/pdf/conduct.pdf.

[34] Association for Computer Machinery. ACM Code of Ethics and Professional Conduct. (October1992). [Online]. Available: http://www.acm.org/constitution/code.html.

[35] B. Bacheldor. AMA Issues Ethics Code for RFID Chip Implants. (July 2007). *RFID Journal.* [Online]. Available: http://www.rfidjournal.com/article/view/3487/2.

[36] M. J. Quinn, *Ethics for the Information Age*; Oregon State: Addison-Wesley, 2005.

[37] U.S. Food and Drug Administration. List of Medical Devices by Product Code. (November 2012). [Online]. Available:http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/UniqueDeviceIdentification/UCM328694.pdf.

[38] J. Fritsch, S. Petronio, p. Helft, A. Torke, "Making decisions for hospitalized older adults: ethical factors considered by family surrogates," *Journal of Clinical Ethics*, vol.24, no.2, pp. 125-134, 2013.

[39] D. Halperin, T. Kohno, T. S. Heydt-Benjamin, K. Fu, W. H. Maisel, “Security and privacy for implantable medical devices” *Journal of Pervasive Computing,* vol.*7*, no.1, pp. 30-39, 2008.

[40] J. Kent. Malaysia Car Thieves Steal Finger. BBC News. (March 2005). [Online]. Available: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.

[41] T. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, T. Ohare, “Vulnerabilities in First-Generation RFID-enabled Credit Cards,” In *Proc. 11th FC Conf.*, 2007, pp. 2–14.

[42] P. P. López, “Lightweight Cryptography in Radio Frequency Identification (RFID) Systems,” Ph.D. Dissertation, Dept. Elect. Eng., Madrid Univ., Madrid, Spain, 2008.

[43] E. Barker, A. Roginsky, NIST Special Publication 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, (2011).

[44] R. L. Rivest, A. Shamir, L. M. Adleman,“ A Method for Obtaining Digital Signatures and Public-Key Cryptosystems,” *Association for Computing Machinery (ACM),* vol. 26, no. 1, pp. 96-99,1983.

[45] S. Barreras, J. Francisco, O. Jimenez. "RF coupled, implantable medical device with rechargeable back-up power source," U.S. Patent no. RE42682. 6, Sep. 2011.

[46] N. Koblitz, “Elliptic Curve Cryptosystems,” *Journal of American Mathematical Society*, vol. 48, pp. 203-209, Jan. 1987.

[47] S. Martínez, M. Valls, C. Roig, J. M. Miret, F. Giné, “A Secure Elliptic Curve-Based RFID Protocol,” *Journal of Computer Science and Technology*, vol. 24, no. 2, pp. 309-318, Mar. 2009.

[48] J. P. Aumasson, L. Henzen, W. Meier, M. Naya-Plasencia, “Quark: A Lightweight Hash”, *Springer Journal of Cryptology*, vol. 26, no. 2, pp. 313-339, Apr. 2013.

[49] J. Daemen, V. Rijmen, *The Design of Rijndael*; Germany: Springer-Verlag, 2002, ch. 3.

[50] T. Okamoto, “Provably Secure and Practical Identification Schemes and Corresponding Signature Schemes,” In *Proc. 11th IC Conf.*, 1992, pp. 31-53.

[51] B. Van Rompay, “Analysis and Design of Cryptographic Hash Functions, Algorithms And Block Ciphers,” Ph.D. Dissertation, Dept. Elect. Eng., Leuven Univ., Leuven, Belgium, 2004.

[52] E. Barker, A. Roginsky, NIST Special Publication 800-131A Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, 2011.

Sanaz Rahimi Moosavi received her B.Sc. (Tech) degree in computer software engineering from the Department of Electrical and Computer Engineering, University of Imam Reza, Mashhad, Iran, 2006, and M.Sc. (Tech) degree in information technology, networked systems security, from the Department of Information Technology and Communication Systems, University of Turku, Finland. Her research interests include Privacy issues in Wireless Networks, Internet of Things (IoT) systems, and Lightweight Cryptography algorithms.

Antti Hakkala received his B.Sc. (Tech) and M.Sc. (Tech) degrees from University of Turku, Finland. He is currently pursuing a doctoral degree in communications engineering at the Department of Information Technology, University of Turku. His main research areas are in the fields of cryptography, biometrics and information security.

Johanna Isoaho received her M.Sc. degree in social sciences from University of Turku in 1993. She has worked multi-professionally for 17 years in the area of social work including different types of positions and organizations. The work has had a wide scope from clients with dual/triple diagnosis to working with rehab groups. Currently she is Ph.D. student at University of Turku researching information security in social and medical processes.

Seppo Virtanen received his B.Sc. in applied physics, MSc in electronics and information technology (1998), and DSc (Tech.) in communication systems (2004) from the University of Turku (Finland). Since 2009, he has been Adjunct Professor of Embedded Communication Systems at University of Turku. He is Editor-in-Chief of the International Journal of Embedded and Real-time Communication Systems and a senior member of the IEEE. His recent research interests have been on platforms capable of handling the processing of communication protocols, DSP routines, and SDR algorithms and applications in parallel on a parameterizable hardware platform, as well as on cyber and information security topics.

Jouni Isoaho received his M.Sc.(Tech) in electrical engineering, and his Lic.Tech. and Dr.Tech. in signal processing from Tampere University of Technology, Finland, in 1989, 1992 and 1995, respectively. Since 1999 he has been the professor of communication systems at University of Turku, Finland, where he heads the communication systems laboratory. His research interests include future communication system concepts, applications and implementation techniques. His current special interests are in dynamically reconfigurable self-aware systems for future communication and interdisciplinary applications including information security and dependability aspects.