INTRODUCTION

Since it was brought forward conceptually in the 1960s, RFID has come a long way to mature before it was rolled out to markets. Fields including transportation management, inventory industry, electronic payment and physical setting access control have already seen implementations of this technology to various extent. As expanding territory is driven under the name of RFID, advocates voice their concerns that the number of RFID in possessions might exceed reasonable bounds and sound the alarm of it being abused. However, it will be too prudent to abandon this promising technology without thoroughly scrutinizing it. This remains true when RFID tags are planned to be injected in subcutaneous position within humans for access control management or even individual GPS tracking. This report primarily evaluates RFID tags against three selected criteria, namely “technical feasibility”, “health and safety” and “security” in terms of human-body implantation. The part of the report which followed will be divided into four sub-parts, with the first three being the evaluation (the main part) of how RFID fulfills the three chosen criteria and the final one constituting a general conclusion.

Ⅰ.TECHNICAL FEASIBILITY

As is known to all, evaluation is unnecessary and daydream-alike when the subject of it is impossible to be achieved. Consequently, the first step of the process is evaluation of technological feasibility (TF). In this section, TF of GPS tracking function will be assessed, then identification and authentication functions. To begin with, GPS real-time tracking is mostly regarded as desirable but impractical by researchers (Azad, Ali, 2009)(Aubert, 2011)(Bakker, 2013). This is because with recent technologies qualified antennas either to receive or to send electromagnetic waves capable of covering such long distances to lock into satellites using batteries or energy-harvesting devices can not yet be designed, partially due to significant attenuation of radio waves through human tissues which mainly consist of water full of ions. In addition, the level of continuous electromagnetic field in the exposed cells surrounding the implanted device may not be able to conform to the legislated security standards if only to satisfy the range and frequency requirements. Moreover, when considering the energy supply, it is perceived that no battery of tag-size is capable of driving the circuitry in useful durations, not even irrechargeable ones, let alone other rechargeable weak batteries or energy-harvesting devices.

When it comes to identification and authentication functionalities, the prospect seems delightful. The Electronic Article Surveillance (EAS) and passive tags with identifier codes have, in fact, been already adopted to detect presence/ absence and identities of objects at large for many years. This type of RFID tags can only be read within a narrowly limited range, when activated by an off-body interrogator with inquiry signals in the form of electromagnetic waves, thus a battery does not have to be integrated, making it completely within reach. As to the tags requiring the ability to send messages e.g. human blood pressure sensors, energy suppliers (either batteries or energy-harvesting devices) are sufficiently endurable. The geometry and polarization of the antennas are worth noting, since in this area of RFID tags lie the most intractable problems. For tags implanted in living individuals, low frequency radio wave is a desirable option for the realization of portable data sensing, because of its property that absorption by flesh is minor thus saving energy without reducing range. If the antenna is made directive, the hyperthermia of tissue in proximity with the tag can be lowered, further facilitating the transmission of

radio waves. To draw a conclusion concerning technological feasibility, passive and short-range info-sending tags are practical, while GPS functionalities may be quite a challenge out of reach for RFID tags.

Ⅱ.HEALTH AND SAFETY

Another noteworthy issue lies within the bounds of post-implantation health and safety. As stated by Albrecht(2010), there seems to be an definite casual link between implanted RFID and tumors in rodents and dogs. According to the literature he studied, almost all of the experiments with reasonably long implantation time and sufficient number of animals observed induced-tumors with differing rates of tumorigenesis, attendant hypotheses of which are given including “1) foreign-body tumorigenesis 2)post-injection sarcoma 3)possible genotoxic properties of the implant and 4)radio-frequency energy emissions from the transponder or reader” (Albrecht, 2010).

To dilate on these four hypotheses, the first hypothesis states that simply the presence of a subcutaneously lodged foreign-body can engender changes of cellular reactions and induce malignant cancers. The likelihood of tumor growth is influenced most significantly by the exterior configuration of the injected foreign-body, with “rough, scratched, and porous surfaces” less likely to give rise to tumors. This is to some degree counterintuitive because a smooth, homogeneous surface is more often associated with shorter span of active inflammation period. Nevertheless, compelling evidence suggests that less extended period of inflammation correlates to a higher rate of cell carcinogenesis instead of lower one.

The second hypothesis seems paradoxical when combined with the first one, providing contradiction. It claims that merely the inflammatory reaction itself, no matter how long it lasts, can stimulates tissues so that they are more vulnerable to tumorigenesis. The induced malignant sarcomas are perceived in veterinary terms as post-injection sarcomas.

The third hypothesis is based on a specific experiment in which genetically modified mice with “exquisite sensitivity to mutational and carcinogenic effects of genotoxic chemicals” experience unexpectedly high rate of developing malignances. Researchers suggest that this could be due to hidden genotoxic qualities in the surface of tags, either that genotoxic byproducts are generated during the process stated above in the first two hypotheses or that “leachates” of the polypropylene polymer sheath into the tissues where the capsule is embedded somehow elicit tumorigenesis.

Th fourth hypothesis is briefly mentioned within the technical feasibility section, describing the possibility that strong enough radio energy of the transponder's signals may be carcinogenic. Not only do surrounding tissues absorb the energy, in view of its electro-magnetic attributes, they probably also get “manipulated” genetically, whose long-term effects are still dark.

Apart from cancers caused by implant, there are other adverse reaction including migration, injection, failure and loss of the transponder etc. likely under-reported. However, a direct leap in deduction from rodent vulnerability to certainly similar human vulnerability should be avoided and the human susceptibility of such adverse reactions, including tumors, should be more comprehensively considered and researched. Thus, this section's conclusion can be drawn that RFID implants may not be totally appropriate for human-bodies in the light of some convincing evidence from laboratories, and further study of such issues are needed before settling down whether it is safe and healthy to embed microchips into human tissues.

III.SECURITY

The term “security” within this report has a dual purpose, serving as both “physical security of the bearers” and “privacy”, the two intimations of which are actually closely correlated. The subsequent part of this section will mainly be based on two articles with Halamka et al (2006) and Ayoade (2006) being authors. The former examined the security properties of Verichip, a commercial passive RFID tag designed to be implanted into human bodies, and the latter proposed one challenge-response scheme for RFID. Conducted by Halamka et al, an attempt to spoof i.e. to forge a Verichip signal was carried out to prove that static radio signal emitter RFID tags like Verichip are very vulnerable to spoofing attacks, either replay attacks or existential attacks. The first type of spoofing can come true with the help of a device that is able to capture and simulate signals conceived from a Verichip by means of clandestine scanning or eavesdropping when the tag is being scanned by a legitimate reader, therefore more undetectable and having longer range. In this way, readers can not distinguish between a valid tag and a spoofing device, in view that no optical images are perceived from them. Apart from signal emulation, actual circuitry duplication admits of another kind of spoof, existential spoofing attacks. As long as the specifications for the Verichips are obtained, one can possibly deploy a commercial off-the-shelf reader to get hands on the ID number of a tag then create a forgery Verichip referring to the specifications. Even if active RFID tag with varying encrypted signal emissions or whatever encoding schemes are designed to overcome the shortcomings at the authentication aspects, concerning physical bearer safety, they are better not implemented in order to preclude potential adversaries from forcefully extracting the unspoofable RFID tags from victims' flesh or coercive attacks on bearers, which are intended to get access to valuable resources or important settings for immediate financial benefits or other ulterior reasons.

Therefore, the authors of the former article argue that RFID tags should only be used as convenient identification devices providing substitution for barcodes, not authentication ones. In regard to the privacy of its bearer, the authentication processing framework, or APF, proposed by the latter article can be implemented to complement the identification function of RFID tags. It in fact involves a database access control system, thus allays the privacy concerns which are virtually connected with the personal information stored in the database. Structured within this conceptual frame, unauthorized readers merely receives or replays the encoded signals from a tag but can not access the vast information linked with the code expressed in the signal due to the fact that the APF will not release the key used to decode it to make it an unkeyed key to the database. This predispose the circumstances on bearers to a

relatively safe one, mitigate the disquieting spectre of automatedly detonated “RFID sniffing bomb” etc. mapping privacy to the actual physical security of a specific individual. (Juels et al,2005)

CONCLUSION

To draw a conclusion at large, RFID tags had better served only as convenient identification devices, not authentication ones, otherwise even the most sophisticated encryption schemes can not assure bearers safety. Passive tags are not out of reach with present technologies, but GPS tracking tags may be impractical for now. As to the health and safety of tag implantation, evidence which can not be ignored indicates that there is a definite casual link between implant and cancers. More uninformed implantations should be immediately halted henceforth until the cancer developing process is better studied. In a word, RFID tags can only apply to limited fields of activities such as substitution for barcodes and ought to be regarded with more caution considering its medical and security properties.