RFID and Privacy Impact Assessment (PIA)

Claude Tételin

Centre National de Référence RFID, ctetelin@centrenational-rfid.com

Mots clés : RFID, privacy, risk assessment, security

1 History of RFID Privacy Impact Assessment (PIA)

Behind the word RFID, we can find several technologies whose characteristics allow considering many diverse applications. In some cases, individuals are directly involved. We can mention the cases of access badges, transport cards, official documents such as e-passports or more recently the introduction of electronic contactless payment cards and NFC. If citizens are not always aware of the information that this kind of application can process or the level of security implemented, they can nevertheless balance the risks and the benefits of such applications. For other applications, individuals are currently excluded from the value chain. We can mention applications, mainly based on UHF technology, devoted to logistics from manufacturers to point of sale. Even if there is no or very little added value for the customer, this does not prevent people from getting stuck with or surrounded by some of these tags. The reason why RFID can cause public distrust and privacy concerns is the combination of two issues: public unawareness and impossibility to switch off RFID devices. That's the reason why, in response to the growing deployment of RFID systems in Europe, the European Commission published in 2007 the Communication COM(2007) 96[1] "RFID in Europe: steps towards a policy framework". This Communication proposed steps which needed to be taken to reduce barriers to adoption of RFID whilst respecting the basic legal framework safeguarding fundamental values such as health, environment, data protection, privacy and security.

Two years later, in May 2009, the European Commission issues a Recommendation 'on the implementation of privacy and data protection principles in applications supported by radio-frequency identification'[2]. This document outlines data privacy objectives recommended for use in the 27 member states. It is proposed that consumers should be informed of the presence of RFID tags placed on or embedded in products, and that tags should be removed or deactivated immediately at the point of sale. The tag can be kept operational only if purchasers expressly agree (Opt-in). However, deactivation could be not systematic if the retailer assesses the privacy and data protection risks.

According to Article 4 of the Recommendation, industry, in collaboration with relevant civil society stakeholders have to develop a framework for privacy and data protection impact assessments. After long and sometimes difficult discussions, but finally endorsed by the Article 29 Working Party in February 2011, the "Privacy and Data Protection Impact Assessment Framework for RFID Applications"[3] has been published.

Meanwhile, in December 2008, the European Commission addressed the Mandate M/436[4] to CEN, CENELEC and ETSI in the field of ICT as applied to RFID systems. The Mandate M/436 was accepted by the ESOs in the first months of 2009. The Mandate addresses the data protection, privacy and information aspects of RFID, and is being executed in two phases. Phase 1, completed in May 2011, identified the work needed to produce a complete framework of future RFID standards. The Phase 1 results are contained in the ETSI Technical Report

[1] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0096:EN:NOT
[2] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
[3] http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf
[4] http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Documents/m436EN2.pdf

TR 187 020[5], which was published in May 2011. Phase 2 is concerned with the execution of the standardisation work programme identified in the first phase. This second phase will end in 2014 with the publication of different technical reports and the publication of two European standards: "RFID Privacy Impact Assessment (PIA) process" and "Notification of RFID: The information sign and additional information to be provided by operators of RFID data capture applications".

The European norm on PIA will be based on the Privacy and Data Protection Impact Assessment Framework for RFID Applications. It will define aspects of that framework as normative or informative procedures to enable a common European method for undertaking a RFID PIA. It will provide a standardised set of procedures for developing PIA templates, including tools compatible with the RFID PIA methodology. In addition, it will identify the conditions that require an existing PIA to be revised, amended, or replaced by a new assessment process.

2 Preliminary considerations

2.1 Privacy

The first key question we have to answer before going deeper in the process is: "What is privacy?" Privacy, as a concept, is always difficult to define with clear boundaries. Depending on the culture and individuals, emphasis can be put on reputation or human rights. Generally accepted by most privacy experts, Alan F. Westin's definition of privacy is commonly used[6]: "the claim of individuals (...) to determine for themselves when, how and to what extent information about them is communicated to others" and as a mean "(...) for achieving individual goals of self realization"

One of the reasons why privacy creates conceptual problems is that different aspects of privacy are belonging to different sectors like data protection (collection, accuracy, protection and use of data collected by an organisation) and data security (protection of collected data). Privacy can generally be discerned into five categories. These types of privacy are covered by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[7].

1) **Physical privacy**. This is to ensure the integrity of the body of the individual. Issues that are more readily associated with privacy include body searches, compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissues, requirements for submission to biometric measurement and compulsory sterilization
2) **Privacy of personal behavior**. This relates to the observation of what individuals do, and includes such issues as optical surveillance also called as "media privacy". This affects all aspects of behavior, including intimacy, sexual behavior, political or trade union activities and religious practices both in private and in public spaces.
3) **The privacy of personal communications**. For individuals, it is important that they can use a variety of media to communicate without their communications being watched by other persons or organisations. This form of privacy is also known as "interception privacy"
4) **The privacy of personal information**. Is referred to variously as "data privacy" and "information privacy". Individuals claim that data about themselves, not necessarily should be automatically available for other individuals and organisations, and that, even though others obtain such data, the individual himself must be capable to exercise a considerable degree of control over these data and the use of these data.
5) **The spatial privacy** as a shield of its own territory.

[5] http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf
[6] Westin, A., 1967, Privacy and Freedom, New York: Atheneum
[7] http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm

2.2 Personal data

The Directives 95/46/EC[8] and 2002/58/EC[9] (privacy directives) are applicable only when the processing of personal data is taking place.

Personal data are defined as any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Processing personal data can then be defined as any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as reading, collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction.

Within an organisation, the controller is responsible that the processing of personal data is performed in compliance with the privacy directives. Of course, RFID, like any other mean of automatic identification and data capture technique, if processing personal data, has to be compliant with the law. This include the tags, the air interface, the interrogators and the connection to the backend system.

Article 17 of 95/46/EC and Article 4 of 2002/58/EC obliges the controller to implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. The measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

When focusing on personal data, it is clear that privacy protection and information security overlap each other but are not similar. That is one of the reasons why the concept of privacy impact assessment (PIA) is more and more widely used. Following the ISO definition of the difference between a PIA and a privacy compliance audit[10]:

> *A privacy compliance audit differs from a privacy impact assessment in that the compliance audit determines an institution's current level of compliance with the law and identifies steps to avoid future non-compliance with the law. While there are similarities between privacy impact assessments and privacy compliance audits in that they use some of the same skills and that they are tools used to avoid breaches of privacy, the primary concern of a compliance audit is simply to meet the requirements of the law, whereas a privacy impact assessment is intended to investigate further in order to identify ways to safeguard privacy optimally.*

It is clear that a Privacy Impact Assessment is not a regulatory compliance audit and, by extension, it is neither a security audit.

2.3 RFID operator

Before entering much deeper in the PIA process, we need to define clearly the concept of RFID operator because he is the only one responsible in undertaking a PIA for the RFID application he intends to set up. The definition is given in the Recommendation[11]:

> *'RFID application operator' or 'operator' means the natural or legal person, public authority, agency, or any other body, which, alone or jointly with others, determines the purposes and means of operating an application, including controllers of personal data using a RFID application*

[8] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1995:281:0031:0050:EN:PDF
[9] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF
[10] ISO 22307:2008, Financial services -- Privacy impact assessment
[11] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

This means that any organisation that carries out a reading (decoding) process on a RFID tag or that carries out a writing (encoding) process on a RFID tag is concerned by the Recommendation and by undertaking a PIA. The question is to know how to undertake a PIA and what is the level of detail requested for a given application.

3 The PIA process

3.1 When undertaking a PIA?

As soon as a RFID operator intends to set up a RFID application, he has to ask the question of undertaking a PIA. The RFID PIA process shall not only deal with the internal context, in terms of all the planned communication between the RFID tag and the business application. The PIA process has to take into consideration the external context, in terms of the RFID tag leaving the organisation's application environment and still being functional. That's why the Recommendation focused on the retail sector where a tag used for internal purpose like inventory, re-assort or anti-theft can go through the point of sale and continue to be functional if not deactivated.

Of course, undertaking a PIA for a brand new RFID application is not the only case. There are other different situations when a RFID PIA has to be considered. A beneficial and cost-effective approach may be to consider the RFID PIA as a continual process which has to be re-visited at each new project phase or new situation.

Given the significant investment that any organisation makes in a RFID application, and the reputation risks of inherent features in the technology not being addressed, there are numerous business advantages in undertaking the RFID Privacy Impact Assessment. These advantages are even greater and easy to demonstrate if privacy concerns have been identified and mitigated before the complete implementation of the RFID application. That's why the European Commission and a lot of privacy experts consultants emphasize the principle of privacy by design.

3.2 Different PIA levels of detail

The PIA Framework suggested four levels of PIA (0 to 4) and explicitly stated "Industry may further refine these levels and how they impact the PIA process with further experience." To know what kind of PIA has to be undertaken, the PIA Framework proposed a simple decision tree based on simple questions like:

> *"Does the RFID application process personal data? OR Will the RFID Application link RFID data to personal data?"*
>
> *"Do the RFID tags used in the RFID Application contain personal data?"*
>
> *"Is it likely that the RFID tags you process are carried by an individual?"*

Answering these questions leads to different PIA scales. Unfortunately, these questions can be differently interpreted and furthermore, the different PIA scales (small or full scale PIA) are not well defined in the PIA Framework. That's why, the future European standard will propose the following definitions:

Level 0 - no PIA: If a RFID tag is not carried by, or is associated with, an individual then the PIA process may stop before entering the PIA process itself and the operator has only to prepare the RFID functional statement.

Level 1 - small scale PIA: If a RFID tag is carried by, or is associated with, an individual on a permanent or temporary basis, then all the PIA process has to be done. Where no asset or associated data type is defined in the category of personal privacy, the remaining risk analysis process is simplified.

Level 2 - PIA of the controlled domain of the application: This level of PIA is required when the application processes personal data, but such personal privacy data is not held on the RFID tag. The risk assessment process for a level 2 PIA is only applied to the part of the application which is controlled by the operator. This does include the communications interfaces between the interrogator and tag, and interrogator and application.

Level 3 - PIA of the controlled and uncontrolled domain of the application: This level of PIA is required when the RFID holds personally identifiable data. The risk assessment process for a level 3 PIA is applied to the controlled part of the application as for level 2. In addition, a risk assessment is required for the data on the RFID tag in the uncontrolled part of the application.

3.3 The PIA process

If, following the proposed defined levels of PIA, the operator has to undertake a PIA (levels 1, 2 and 3), he can follow the 9 steps defined in forthcoming European standard:

STEP 1 Prepare a detailed description of the application.

STEP 2 Identify and assign a risk value to the privacy assets as follows:

- the personal privacy assets of an individual in possession of a RFID tag used by the RFID application, and also in the individual's possession beyond the bounds of the application;
- the organisation's assets that might be implicated with a privacy breach or loss of personal data associated with RFID data processing.

STEP 3 Identify and assess the threats to the privacy assets. This applies to individual assets beyond the domain on the application, i.e. ensuring the privacy protection is addressed. It also applies, and is linked to, threats to sets of personal data held by the RFID operator / data controller.

STEP 4 Identify the vulnerabilities associated with the threats and assets.

STEP 5 Carry out a risk assessment of the assets, where risk is a function of (asset, threat, vulnerability), taking account that there can be a number of risks.

STEP 6 Identify existing and new controls that can be applied to mitigate risks.

STEP 7 Determine the residual risks. If assessed too high re-start form step 2.

STEP 8 Complete and sign-off the RFID PIA report.

STEP 9 Complete and sign-off the RFID PIA summary report to be made available in the public domain.

Steps 2 to 7 are considered as the risk assessment process. Operators have to be careful of what they consider to be personal data and have to refer to clause 2.2 of this document.

3.3.1 Identifying and ranking privacy assets

Referring to different aspects of privacy defined in 2.1, identifying privacy assets is not an easy task. It much more easier to refer to the data processed by the RFID application. All the data either processed in the back-end system or stored directly into the memory of the RFID tag have to be considered. The type of data can then be linked to a particular privacy asset. Two categories of assets have to be identified as appropriate for the application, based on the type or implication of the data on the RFID tag or stored on the application:

- Directly identifiable assets, where encoded data includes:
  - An individual's name
  - A unique chip ID
  - Any identifier that has a one-to-one relationship with the individual
- Indirectly identifiable factors specific to the individual's physical, physiological, mental, economic, cultural or social identity, as included in Directive 95/46/EC for the definition of personal data.

Using a sector-based or application based PIA template or starting from scratch, the operator has to use the full description of the RFID application prepared in step 1 to identify all the relevant privacy assets. The next work is to classify assets and sort them by order of importance. Depending on the PIA level and organisation's size, most relevant or all identified assets will have to be considered.

3.3.2 Identifying and ranking threats

As for privacy, we can find a lot of definition of a threat depending on whether we integrate or not the agent, his motivation and sometimes a piece of vulnerability. The one we propose in this document is derived and adapted from ENISA[12]:

> *physical, hardware, or software mechanism with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data and / or denial of service*

Of course, the identification of threats for a RFID application has to consider:

- technological aspects like the data encoded in a tag, the air interface protocol, the device interface and the application layer
- security aspects like confidentiality, integrity and availability

Like for privacy assets, all identified relevant threats have to be sorted by importance. Among others, we can cite the most known RFID threats: tag cloning, eavesdropping, man in the middle, denial of service, malicious code, etc. For a more complete list of threats, the reader may refer to the M436 phase 1 report[13] or to the forthcoming European standard on PIA.

In the evaluation of threats, it is important to take into account the motivation and the required skills of the attacker. The probability of such an attack is another important criterion.

3.3.3 Identifying and ranking vulnerabilities

Like for threats, it is important to have a definition of vulnerabilities. Among others, the one proposed by Information Technology Security Evaluation Criteria[14] (ITSEC) is:

> *The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.*

Another way to identify RFID vulnerabilities is to evaluate the use or not of special features like kill command, read/write password protection, untraceable command, use of particular cryptographic algorithms, etc. The goal of the PIA process will be to identify the vulnerabilities and to assess the risk. One way of mitigating the risk will be to use these kind of features. A more complete list of vulnerabilities can be found in the M436 phase 1 report.

For scoring the vulnerabilities, the operator can use the following rules:

1) If it is impossible to implement a threat, then the vulnerability risk level shall be defined as 'low'. For example, a crypto attack cannot be implemented on an RFID tag and air interface protocol that does not support cryptographic features. If the threat is possible, then the criteria set out in the next step apply.

2) If a threat is identified and if it is feasible to apply this to the RFID technology used in the application, then its vulnerability risk level shall be 'medium' to indicate that the threat and implied vulnerabilities have been identified in research documents.

3) The vulnerability level of 'high' shall only be applied when known exploits have been identified in real applications.

[12] http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/glossary
[13] http://www.etsi.org/deliver/etsi_tr/187000_187099/187020/01.01.01_60/tr_187020v010101p.pdf
[14] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile

3.3.4 Risk evaluation

Once the assets, the threats and the vulnerabilities have been identified and ranked, the last step is the risk assessment. Different methods can be used to assign a value to a given risk. We can cite here the OCTAVE[15] method developed by Carnegie Mellon University in 2001. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a suite of tools, techniques, and methods for risk-based information security strategic assessment and planning. Another method is the DREAD algorithm where the value of the risk is derived from the equation: Risk_DREAD = (Damage + Reproducibility + Exploitability + Affected users + Discoverability) / 5. Another method is proposed by NIST in the special publication 800-30[16]. All these methods and scoring algorithms are more or less devoted to computer security and are not well suited to privacy risk assessment. In this paper, and in the future European standard, we propose a method based on the ISO/IEC 27005:2011[17] standard. In this method, assets can have a value between 0 and 5. For threats and vulnerabilities, values are whether low, medium or high. The equation that gives the risk value is based on the addition of asset, threat and vulnerability values and can be summarised in the table below. Of course, the higher the number, the more serious the risk.

	Likelihood of Threat	Low			Medium			High		
	Ease of Exploitation - Vulnerability	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Table 1 - Matrix approach to determine a risk value based on ISO 27005

3.3.5 Mitigation and controls

Each operator has to define his own threshold for risk value that imply an action to be done. If one or more risks have a value above this threshold, the operator has to mitigate the risk by implementing a countermeasure. Countermeasures can be classified as follow:

- features embedded in the tags and devices associated with a particular air interface protocol.
- features available in the technology but require a conscious action by the RFID operator.
- features independent of the hardware and can be implemented by the RFID operator.
- action that the individual has to do to protect his or her privacy.

Once one or more controls have been implemented, the operator has to re-assess the risk value and verify that this time, the value is below the threshold he decided to set.

3.3.6 Residual risks

It is generally agreed upon RFID stakeholders that a zero privacy risk RFID application is something that cannot be achieved. Depending on the threshold defined by the operator, there still are risks that have not been

[15] http://www.cert.org/octave/octavemethod.html
[16] http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
[17] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742

mitigated. These are called residual risks. This concept is defined in ISO Guide 73:2009, Risk management – Vocabulary[18]: Risk remaining after risk treatment.

Of course, the lower the value of residual risks, the higher the confidence of individuals in the RFID application. The RFID operator has to calculate the ROI of the implementation of even more controls and countermeasures.

3.3.7 The PIA report and summary

Once the risk assessment has been completed, the final resolution about the application should be documented in the PIA Report, along with any further remarks concerning risks, controls and residual risks.

Those signing off should have the necessary skills to understand the RFID application and/or have the authority to require a system change should this be necessary.

Such PIA report may contain confidential information on how RFID is implemented by a given operator. In order to communicate with involved stakeholders out of the organisation, the operator has to draft a PIA summary report. This summary shall at least include: the PIA report date, the name of the RFID operator, the RFID application overview, the data embedded in the RFID tags, the RFID privacy impact assessment score (derived from Table 1), RFID controls and mitigations.

As it has been said earlier, PIA is a continual process which has to be re-visited at each new project phase or new situation. The criteria for a review may include:

- Significant changes in the RFID application such as expanding on the original purpose.
- Changes in the type of information process either as held on the tag or on the application.
- Reports of privacy breaches in similar RFID applications.
- The availability of a new or enhanced sector template.
- The availability of improved RFID technology. However, it is acknowledged that the residual value of existing investments and the migration to the new technology need to be taken into consideration.
- Periodically; ideally no more than one year should elapse, the existing PIA should be re-assessed. If no material changes have occurred, then all that is required is to indicate this fact with an updated date.

4 Conclusion

The work done by the European Commission and numerous industrial and academic stakeholders on privacy related to RFID application can be seen as a first step to promote smart and privacy friendly use of RFID. For the moment, the Recommendation is what we can call a soft law. The PIA Framework is a first attempt to propose a defined process to RFID operators. It allows RFID operators to assess how the application can harm individual's privacy and help them in indentifying ad hoc controls and mitigation methods.

We can often ear that RFID is not the most dangerous technology for privacy. Never mind, the RFID operators have now the opportunity to set up an example and induce other sectors. The forthcoming European standard will surely help RFID operator even more by a well defined set of procedures and steps. Such a standard can help to implement a repository for ensuring compliance. Such compliance, across Europe, will lead to greater confidence from the citizens towards RFID. This, seen by an organisation like French RFID National Centre, is the best reward that an operator and by consequence all RFID manufacturers, can obtain.

[18] http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=44651