RFID Security and Privacy

Michel Arnaud

RFID Security and Privacy

Prof. Michel Arnaud
University Paris Ouest Nanterre la Défense

Introduction

The European Commission has published in May 2009 a recommendation "*on the implementation of privacy and data protection principles in applications supported by radio-frequency identification"*, which is designed to provide "*guidance to Member States on the design and operation of RFID applications in a lawful, ethical and socially and politically acceptable way, respecting the right to privacy and ensuring protection of personal data*." This recommendation requires RFID operators to conduct a "Privacy and Data Protection Impact Assessment" before any RFID application is deployed, and make its results available to the competent authority. The RFID recommendation is also designed to promote "*information and transparency on RFID use"*, in particular through the development of "*a common European sign developed by European Standardisation Organisations, with the support of concerned stakeholders",* designed "*to inform individuals of the presence of readers"*.

RFID PIA (Privacy and Impact Assessment) process aims to reach several objectives:
• to favor "privacy by design" by helping data controllers to address privacy and data protection before a product or service is deployed,
• to help data controllers to address privacy and data protection risks in a comprehensive manner, an opportunity to reduce legal uncertainty and avoid loss of trust from consumers,
• to help data controllers and data protection authorities to gain more insight into the privacy and data protection aspects of RFID applications.

The industry has proposed a RFID PIA framework which classifies a RFID application into 4 possible levels:
-Level 0: applications that do not process personal data and where tags are only manipulated by users, and which are rightly excluded from conducting a PIA.
-Level 1: applications where no personal data is processed, yet tags are carried by individuals.
-Level 2: applications which process personal data but where tags themselves do not contain personal data.
-Level 3: applications where tags contain personal data.

If the RFID application level is determined to be 1 or above, the RFID operator is required to conduct a four part analysis of the application, with a level of detail that is proportionate to identified privacy and data protection implications. The first part is used to describe the RFID application. The second part allows highlighting control and security measures. The third part addresses user information and rights. The final part of the proposed PIA framework requires the RFID operator to conclude whether or not the RFID application is ready for deployment. As a result of the PIA process, the RFID operator will produce a PIA report that will be made available to the competent authority.

For the industry, only levels 2 and 3 are to be submitted to a PIA because it considers that information contained in a level 0 tag are not personal. However level 1 rises concerns of Article 29 Working Party because tagged items carried by a person contain unique identifiers that could be read remotely. In turn, these unique identifiers could be used to recognize that particular person who will be tracked by a third party without her knowledge. When a unique (or multiple identifiers) is associated to a person, it falls in the definition of personal data set forth in Directive 95/46/EC, regardless of the fact that the "social identity" (name, address, etc.) of the person remains unknown (i.e. she is "identifiable" but not necessarily "identified"). Additionally, the unique number contained in a tag can also serve as a means to remotely identify items carried by a person, which in turn may reveal information about social status, health, or more. Even in those cases where a tag contains solely a number that is unique within a particular context and without additional personal data, care must be taken to address potential privacy and security issues if this tag is going to be carried by persons. The Working Party has urged the industry to fully address this issue, by clearly mentioning it as part of a revised risk assessment approach for level 1.

This chapter will address issues of protecting privacy of RFID tag carriers in a "privacy by design" model which is described below on four different layers: legal aspects, policy services, technical specifications and security services. The idea is to provide easy-to-use tools to accept or not to be tracked at PIA level 1. In case of a negative decision, tags have to be deactivated. Authentication techniques are to be used to protect user identity for PIA levels 2 and 3. Security measures have also to be taken to protect personal information on RFID tags against information leak which could lead to identity theft.

Legal framework

Personal data is 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 their physical, physiological, mental, economic, cultural or social identity. Personal data exist in many digital forms and are included in browsers as certificates; mobile phones are generally related to an individual; home, appliances and clothing may include technology (e.g. smart metering, Internet of Things and RFID) which represent owner or user's identity; social networking sites reflect personal information in great detail including : digital information stored in databases, video, pictures, documents, files, notebooks, invoices, medical records, RFID, ID cards, passports, cookies, flash objects, eID middleware, biometric identifiers (e.g. fingerprints, DNA, etc.).

Basic principles of Directive 95-46 of the European Parliament include the following regarding protected data: fairly and lawfully processed, for limited, adequate, relevant and not excessive purposes, accurate and up to date, not kept for longer than necessary, processed in line with individual's rights, secure in processing, storage and transfer, not transferred to other countries without an adequate level of protection.

Identity management

The concept of "identity management" is not well defined with reference to currently available international standards, although there is relevant work in ISO/IEC JTC1/SC27/WG5 *"Identity management and privacy technologies".*

An individual during its lifetime may have many multiple different personae, i.e. names, depending on the roles that it has or qualifies for. For example, at the time of marriage an individual may acquire and use a new (legal) persona. Consequently, an individual may have multiple legally recognized names (LRNs), recognized individual names (RINs), recognized individual identities (riis) at the same time (and so used in various business transactions). Examples include a persona which an individual assigns to himself and is one which also serves as an identifier such as an e-mail address (on a hotmail or gmail account, Facebook, Twitter, as an "avatar", etc.).

A recognized individual name is any persona associated with a role of an individual which is recognized as having legal status, i.e., if a legally recognized name (LRN) is recognized in a jurisdictional domain and accepted in compliance with the registration corresponding schema. Associated with a registered individual name is (usually) a registration number of the document attesting that the RIN has legal status of some kind. A registration authority shall assign a unique identifier to each of its registered members including and especially identifying where the member is acting as an individual. This unique identifier has the properties and behaviors of an ID code in the coded domain

used to support management and maintenance of the registration authority schema.

From an eBusiness perspective, one often does not need to distinguish whether the entity which is party to a business transaction is a "natural person" or "legal person", or an "individual" or "organization", etc. Credit worthiness, ability to pay, secure payment, etc., of a "person", as a buyer, is often a more important criterion for doing business with the person in the role of seller based applications, business (including e-commerce, e-government, e-health, etc.). This is particularly so when modeling Open-edi scenarios and scenario components from an internal constraints perspective only. In much of consumer trade, a buyer can remain anonymous vis-à-vis a seller by presenting a money token in which a seller has 100% trust (e.g., cash).

Privacy protection requirements have made “anonymity” an external constraint matter which needs to be supported. At times it is desired that an individual can establish a long-term relationship (including a reputation, trust relationship, etc.), with some other person, without the individual’s actual identity being disclosed. For convenience, it may be useful for the individual, or the other party concerned, to establish a unique (new) persona, identifier, token, etc., known as “pseudonym” with the other person. Pseudonymization is recognized as an important method for privacy protection of personal information. Pseudonymization techniques, mechanisms and services may be used within an organization or public administration, within a jurisdictional domain as a whole or across jurisdictional domains for transborder data flows.

The following set of rules summarizes privacy protection requirements which apply. A buyer (and its agent(s)) or third party (or any other party to the business transaction), shall not retain any personal information on the individual as the buyer for any time longer than is consented to by the individual for post-actualization purposes unless external constraints of the applicable jurisdictional domain requires retention of such personal information for a longer period.

Good practices

Good practices have been defined within the CEN/ISSS Workshop on Data Protection and Privacy (WS/DPP). Organizations should appoint a person who periodically checks whether notified information is still complete, accurate and up-to-date, or whether grounds for exemption are still valid. The principal purpose of having notification and a public register is transparency and openness. It is a basic principle of data protection that the public should know who is carrying out the processing of personal information as well as other details about processing. Notification, therefore, serves the interests of

individuals by helping them understand how personal information is being processed by data controllers.

Data subject has the right of access, rectification, erasure, blocking and objection to retention. Data controller should respect these rights. Under Section 3 of the Directive, data subjects have the right to find out, free of charge, if any entity (either an individual or an organization) holds information about them. They might also request a description of the information and inquire about the purpose(s) for holding their information.

Anyone having access to the organization's documents, media, computers or information systems is responsible for complying with the information security policy and all other associated documentation that is applicable to it. The information security policy will preserve an appropriate level of confidentiality, integrity, availability, lawful purpose. Support contractors who have access to sensitive information in paper, electronic or other format should sign a written agreement stating they will comply and adhere to organization's policies to keep information secure. Their compliance should be monitored to verify they adhere to these obligations.

PIA framework for RFID

A privacy impact assessment (PIA) enables organizations to anticipate and address likely data protection impacts of proposed initiatives and foresee problems. This process reflects measures taken to protect privacy of individuals about whom sensitive data are kept and addresses legal obligation to use appropriate security measures. Systems should be designed to avoid unnecessary privacy intrusion and with privacy-by-design features implemented to reduce possibility or effects of a security incident.

Individuals responsible for data protection (including their processing service provider) should be identified in the security policy. These documents identify roles, individual responsibilities, incident handling and reporting practices that have been put in place to protect personal data and their processing with appropriate technical and organizational measures to ensure, that at all times, integrity, confidentiality and availability of personal/sensitive data.

The PIA Framework for RFID of January 12, 2011 explains key concepts, internal procedures and classification criteria for RFID applications. For these criteria the PIA Framework provides a two phases approach. The initial analysis phase is used to determine if a PIA of RFID application is required. The decision, to which level an application belongs, has to be made after working

through a decision tree where level 1 implies a small scale PIA while levels 2 and 3 require a full scale PIA. If an application is designed according to level 0 which means that no private data are concerned, there is no privacy threat given and further documentation is not needed. Level 2 applications may have controls to protect back-end data while level 3 applications may have controls to protect both back-end data and tag data. For level 1 applications, required controls and corresponding documentation in the PIA report are simplified.

The objective of the risk assessment phase is to document how risks are pro-actively mitigated through technical and organizational controls. The PIA process requires any RFID application operator to:
1. Describe the RFID application;
2. Identify and list how the RFID application under review could threaten privacy and estimate the magnitude and likelihood of those risks;
3. Document current and proposed technical and organizational controls to mitigate identified risks;
4. Document the resolution (results of the analysis) regarding the application.
The risk assessment requires evaluating the applicable risks from a privacy perspective. The RFID operator should consider:
a. The significance of a risk and the likelihood of its occurrence.
b. The magnitude of the impact should the risk occur.
The resulting risk level can then be classified as low, medium or high. A prime risk is that RFID tags could be used for profiling and/or tracking of individuals. In this case RFID tag's information – in particular its identifier(s) – would be used to re-identify a particular individual. Retailers who pass RFID tags on to customers without automatically deactivating or removing them at checkout *may* unintentionally enable this risk. A key question, though, is whether this risk is likely and actually materializes into an *undismissable* risk or not.

According to recommendation, retailers should deactivate or remove at the point of sale, tags used in their application unless consumers, after being informed of the policy in accordance with this framework, give their consent to keep tags operational. Retailers are not required to deactivate or remove tags if the PIA report concludes that tags that are used in a retail application and would remain operational after the point of sale do not represent a likely threat to privacy or protection of personal data.

The RFID operator should use categories below to indicate privacy and data protection implications of the RFID application:

-Ready for deployment: the RFID application as described provides for suitable practices, controls, and accountability.

-Not ready for deployment: the RFID application is not approved for operations in its current state. A specific corrective action plan has to be developed, and a new privacy impact assessment has to be performed and documented to determine if the application has reached an approvable state.

The PIA Framework provides only a generic scheme for the PIA and has to be complemented by more detailed schemes like roles, security targets, classes and templates reflecting the special aspects of industry-specific and individual applications.

Technical guidelines as templates for PIA

The approach of the European Commission suggests using so-called templates as extensions to the Framework document in order to reach the level of detail that is necessary to conduct a complete application-specific Privacy Impact Assessment. Such templates are specific to an application area and should provide a detailed guidance for the creation of a PIA report. This puts the "Technical Guidelines for the Secure Use of RFID" (TG RFID) into perspective which have been issued by Germany's Federal Office for Information Security (BSI). In 2007 the BSI launched this project which aims at providing technical recommendations for RFID systems that ensure secure implementations and protection of personal data but nevertheless support RFID operators' and service providers' business needs. The BSI achieved a consensus between supporters and critics. TG RFID are accepted by relevant parties and are now available for application areas: public transport, event ticketing, NFC-ticketing, retail & logistics and employee cards. First implementations proved practicality and viability of this approach.

A major goal of development for the TG RFID is to find a consensus and to gain acceptance of all relevant stakeholders. Therefore the BSI installed an intense review and alignment process and invited experts and relevant stakeholders from specific application area to participate. Representatives of RFID operators, service providers, customers, Data Protection Agencies (DPAs) and also critics of RFID have had the opportunity to comment early versions of the document and take part in review and alignment sessions. In this process, security goals, potential threats, security measures and especially remaining risks were identified, discussed and described. This process provided information on potential impact and risks of RFID applications and generated transparency that is necessary to build trust and acceptance. So far Technical Guidelines for five application areas have been created. In all cases a consensus including acceptance from participating DPAs was achieved.

Unfortunately, TG RFID for logistics and retail have not been piloted so far, because progress with RFID in this sector is far behind former projections by retail stakeholders. RFID tags are actually mostly used on pallets and cartons. Products in supermarkets shelves are still only marked with traditional bar codes or with GS1 data bar, except cases like Gillette razors. Whereas in the sectors of ticketing, NFC (13.56MHz) and employee cards (125 kHz HID) a great progress with RFID is on its way.

TG RFID provide patterns for application specific templates which can be efficiently set up as required by PIA Framework.

Stakeholders of an application have individual and sometimes diverging requirements for a technical guideline. Data Protection Agencies (DPAs) want to protect data and privacy of citizens, customers and employees. TG RFID address their objectives by a detailed description of all relevant threats, appropriate safeguards and potentially remaining risks. Operators are focused on their business objectives. Their intention is on practicality, acceptance of their customers and a cost efficient and future proof solution. Balance between objectives of both parties is achieved by a scalable definition of safeguards. Minor threats are mitigated by simple, low-cost safeguards. Strong and costly controls are only applied in case of high protection demand and severe threats. This approach makes sure that cost of security measures and impact on usability are reduced to what is necessary.

Interoperability is an imperative for RFID implementations. Operators need to cooperate with business partners and customers want to use services from multiple service providers and across borders. This requires standardized and interoperable technical interfaces and security measures. In addition, comparability of security levels is of major importance. Operators can only cooperate if they can trust partner's system implementation. This includes a certain level of data protection, privacy and as well information security and safety. TG RFID support these fundamental requirements by two dedicated features:

I. TG RFID include not only an assessment of privacy and data protection. In addition, a risk analysis and documentation of information security and safety is provided. The latter is mandatory to cover business requirements of operators.

II. Risk assessment methodology and documentation of results comply with worldwide standard ISO27005. This makes it easy to compare PIA and security assessment reports of different implementations and systems.

Operators will refrain from investing in RFID applications if they can't determine the cost of security measures and their potential impact on services and usability. Both aspects have major influence on the overall business case. TG RFID define appropriate technical safeguards for specific scenarios of an application. This information builds a solid base for cost calculations and tenders. This feature of TG RFID counters a major roadblock for introduction of RFID.

The European Commission identified lacking confidence in legal situation for RFID-implementations as one major roadblock for the broad adoption of RFID. Use of TG RFID is not mandatory in a legal sense. Nevertheless they will provide a solid basis for legal judgments of RFID applications because they are accepted by all stakeholders and represent the current state-of-the-art for implementations of RFID.

Description of structure and security methodology of TG RFID

TG RFID are created for specific application areas and consist of three major parts: the description of the application area, the assessments and the recommendations. A detailed but generic description of all service and business models of an application area is given in the first part. This is the foundation for assessments and recommendations and covers role models, services, products, business processes, use cases and any other information that may be relevant for security and privacy assessments. In order to ensure practicality and usability for all service providers and operators, this part is done in close cooperation and alignment with experts from the application domain.

The assessment part is based on description of application area and specific security targets. It covers all three domains of information security: security, privacy and safety. Security targets are defined and aligned with all stakeholders. Methodology of risk assessment is compliant with ISO 27005. Results of assessment are a list of relevant threats, appropriate safeguards that can mitigate these threats and a description of remaining risks.

The third part of guidelines document provides recommendations on how to implement an RFID-system in an appropriate way. Based on example scenarios from the application domain it is shown how findings of risk assessment are transformed into specific safeguards that should be applied to the relevant system components. This provides a clear and economically viable guidance for the design of system.

Organizations must be able to demonstrate that they have implemented a data protection management system (DPMS) using appropriate technology (PETs)

and operational protective measures (OPMs) to protect personal data. PIAs incorporate tests of PETS and OPMs to prove data protection principles are met by the system. All personnel within the organization have a responsibility to ensure that they take steps to safeguard security of information that they are entrusted with and to use OPMs and PETs as established policy.

Privacy framework models

OASIS Privacy Management Reference Model (PMRM)

OASIS Privacy Management Reference Model (PMRM) Technical committee aims at achieving a standard-based framework that will help business process engineers, IT analysts, architects, and developers implement privacy and security policies in their operations. PMRM picks up where broad privacy policies leave off. Most policies describe fair information practices and principles but offer little insight into actual implementation. PMRM provides a guideline or template for developing operational solutions to privacy issues. It also serves as an analytical tool for assessing the completeness of proposed solutions and as the basis for establishing categories and groupings of privacy management controls.

This model is based on a service-based approach, describing them in three categories:

- core policy services : agreements (with options and permissions), control (with policies and data management),
- presentation and lifecycle services : interaction (manages data/preferences/notice), agent (software that carries out processes), usage (data use, aggregation, anonymization), access (individual review/updates to personal information),
- privacy assurance services : certification (credentials, trusted processes), audit (independent, verifiable accountability), validation (checks accuracy of personal information), enforcement (including redress for violations)

Personal information is stored in a container accessed by an agent (at entry point) for specific processing which must abide to privacy rules (referred to as agreement and control procedures). Assurance service guarantees conformity to these rules which can be a simple validation or a certification, leading eventually to an audit and an enforcement procedure.

Each use case invokes a sequence of service calls. Each service call executes a sequence of functions: define (operational requirements), select (input, process, and output) data and parameters, input (data and parameter values in accordance with select), process (data and parameter values within functions), output (data,

parameter values and actions), link to other services, secure with appropriate security functions.

Open Identity Exchange Trust Framework

In the context of digital identity systems, a trust framework is a certification program that enables a party who accepts a digital identity credential (called the relying party) to trust the identity, security, and privacy policies of the party who issues the credential (called the identity service provider) and vice versa. In the Open Identity Trust Framework (OITF) model, an open identity trust framework provider can administer any trust framework that meets: 1) the principles of openness, and 2) any additional requirements imposed by the Trust Framework Provider (TFP).

The rules of every trust framework are defined for a particular set of participants in online (and possibly offline) interactions. The Open Identity Trust Framework Model defines six standard trust framework roles (in addition to the trust framework provider role played by OIX):
1. Users
2. Identity service providers
3. Relying parties
4. Assessors
5. Auditors
6 . Dispute resolution service providers
7 . In addition, OIX has defined a seventh role, special assessor, which is an assessor responsible for assessing the qualifications of other assessors.

As defined in the Open Identity Trust Framework Model, a level of assurance (LOA) is a unit of measure for the degree of confidence a relying party can have in assertions for an identity credential from an identity provider. A level of protection (LOP) is a unit of measure for the degree of confidence: a) an identity provider can have in the protection provided by a relying party for the identity information disclosed in an identity credential, or b) a user can have in the protection provided by an identity provider and/or a relying party for the identity information disclosed in an identity credential.

Technical profiles

A technical profile is a specification of requirements for use of a specific technology, RFID in our case, in order to achieve technical interoperability in exchange of digital identity credentials that is consistent with associated LOA or LOP. Once an OIX trust framework is accepted for listing in the OIX Listing

Service, participants may apply for certification.

For RFID open identity trust technical profile, four main functions have to be taken into consideration to provide appropriate tools for agents: anonymization and pseudonymization facilities, attributes management tools, identity management tools, security management tools.

Conclusion

All TG RFID follow a common security concept. Whereas RFID Recommendation is primarily directed towards privacy and data protection, TG RFID cover all three security domains: safety, security and privacy. Furthermore, TG RFID provide detailed guidance how to carry out all detailed work PIA Framework leaves out, because it is understood as a high level document more for senior management and non-IT people. TG RFID are written for IT experts who are responsible for designing systems, investigating threats and weaknesses and providing for the right protection provisions. Definition of generic controls and proposition of scenario-specific safeguards are carried out as a joint approach. This reflects the fact that threats for privacy are often threats to information security as well. Vice versa certain safeguards can counter threats for privacy and information security. The approach of TGs optimizes the impact of safeguards and minimizes cost of security and privacy and complements PIA Framework.

TG RFID provide guidance and information that will enable operators to conduct a PIA and minimize efforts for completing the report. Major parts of the PIA can simply be covered by referencing appropriate chapters as templates and selecting particular services, processes and scenarios mentioned in the guideline. This will work out in most cases because TG are describing all known eventualities of an application area. The operator's application will normally be a subset of what is documented. Furthermore TG RFID provide detailed patterns to develop templates as required by the PIA Framework. All this brings quality of compliance statement to a level that can be trusted by all parties that will deal with RFID-based systems.

Bibliography

Privacy and Data Protection Impact Assessment Framework for RFID Applications
12 January 2011
http://www.statewatch.org/news/2011/feb/eu-art-29-wp-rfid-opinion-annex.pdf

Industry Proposal Privacy and Data Protection Impact Assessment Framework for RFID Applications
March 31 2010
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_annex_en.pdf

Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications
Article 29 Data Protection Working Party
00066/10/EN WP 175
July 13, 2010
http://www.statewatch.org/news/2011/feb/eu-art-29-wp-rfid-opinion.pdf

Technical Guidelines RFID as Templates for the PIA-Framework, Federal Office for Information Security (BSI) Bonn, Germany, 2010.
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG03126/TG_RFID_Templates_for_PIA_Framework_pdf.pdf?__blob=publicationFile

Glossary

Individual anonymity. The state of not knowing the identity or not having any recording of personal information on or about an individual.

Anonymization process. Whereby the association between a set of recorded information (SRI) and an identifiable individual is removed.

Information Security. Preservation of the confidentiality, integrity and availability of information.

Monitor. Carrying out an activity for the purpose of detecting, observing, copying or recording the location, movement, activities, or state of an individual.

Personal Data. 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.

RFID Application. An application that processes data through the use of tags and readers, and which is supported by a back-end system and a networked

communication infrastructure.

RFID Application Operator. 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 an RFID Application.

Radio Frequency Identification (RFID). The use of electromagnetic radiating waves or reactive field coupling in the radio frequency portion of the spectrum to communicate to or from a tag through a variety of modulation and encoding schemes to uniquely read the identity of a radio frequency tag or other data stored on it.

RFID Reader. A fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or reactive field coupling to stimulate and effect a modulated data response from a tag or group of tags.

RFID Tag or 'tag'. An RFID device having the ability to produce a radio signal or an RFID device which re-couples, back-scatters or reflects (depending on the type of device) and modulates a carrier signal received from a reader or writer.

RFID Tag Information or information on the RFID Tag. The information contained in an RFID Tag and transmitted when the RFID Tag is queried by an RFID Reader.

User. Specifically, an RFID Application User, i.e., a person (or other entity, such as a legal entity) who directly interacts with one or more components of an RFID Application (e.g., back-end system, communications infrastructure, RFID Tag) for the purposes of operating an RFID Application or exercising one or more of its functions.