JRC SCIENTIFIC AND POLICY REPORTS

RFID Tags
Privacy Threats and Countermeasures

Current Status

Gianmarco Baldini, Jan Loeschner,
Vincent Mahieu, Ricardo Neisse,
Stefan Scheer, David Shaw,
Luigi Sportiello

2012

Joint
Research
Centre

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information
Jan Loeschner
Address: Joint Research Centre, Via Enrico Fermi 2749, TP360, 21027 Ispra (VA), Italy
E-mail: jan.loeschner@jrc.ec.europa.eu
Tel.: +39 0332 78 5242

http://www.jrc.ec.europa.eu/

JRC 78156

Luxembourg: Publications Office of the European Union, 2012

Printed in Ispra (Italy)

Acknowledgement

The authors would like to thank the following Commission colleagues for their initial impulsion to this project.

Gerald SANTUCCI	DG CNECT
Olivier BRINGER	DG CNECT
Florent FREDERIX	DG CNECT
Jean-Pierre NORDVIK	DG JRC
Laurent BESLAY	DG JRC

European Commission
Joint Research Centre – Institute for the Protection and Security of the Citizen

Title: RFID Tag Privacy Threats and Countermeasures: Current Status

Authors: Gianmarco Baldini, Jan Löschner, Vincent Mahieu, Ricardo Neisse, Stefan Scheer, David Shaw, Luigi Sportiello

Luxembourg: Publications Office of the European Union

2012 – 51 pp. – 21.0 x 29.7 cm

Abstract

In May 2009 the Commission adopted a Recommendation on the data protection, privacy and security aspects of RFID-enabled applications. The RFID Recommendation gives particular attention to the concern about individual tracking and access to personal data in the retail sector, where it is feared that tagged items bought by individuals could be misused by retailers or third parties for tracking or profiling purposes. It establishes the principle that tags must be deactivated at the point of sale unless the customers give their informed consent to keep tags operational. The Recommendation requests the drafting of a "report on the implementation of [the] Recommendation, its effectiveness and its impact on operators and consumers". This refers to the use of RFID in the retail trade in which the deactivation of a RFID tag should become mandatory unless the customer – upon explicit instruction – agrees on keeping the tag activated.
In this context, DG CNECT, within a joint effort with JRC, asked for the identification of best available techniques for deactivating tags at the point of sale in the retail sector. These techniques should obviously be privacy-, data protection-, and security-friendly, but also be economically viable to provide EU companies with a competitive advantage on the global RFID marketplace.
The report summarizes the application of RFID Tags in the retail sector and illustrates associated Privacy Issues and Related Countermeasures. It associates available RFID deactivation techniques with 5 retail scenarios and discusses the privacy of deactivation techniques related to these scenarios.

Table of Contents

1. Introduction

Citizens – while interacting in an increasingly digital world – are more and more leaving their digital traces – mostly in an unconscious way – to third parties (other persons, commercial companies). With these circumstances there is a tendency to (commercially) exploit citizens' data; on the other hand, citizens may become vulnerable as their privacy or integrity may be hampered.

One quite specific application (see also Internet of Things) is the use of RFID chips in high-quality industrial products. Such chips are integrated in a product in a rather invisible way. Benefits of this application lie within the non-reproducibility of that particular product thus making that particular product unique and in particular also traceable; however, with this application, the product (and together with it the citizen who belongs or uses that product) becomes also traceable.

It is clear that rights and obligations concerning the protection of personal data and the free movement of such data (as provided by Directive 95/46/EC [64]) on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 2002/58/EC on privacy and electronic communications are fully applicable to the use of RFID applications that process personal data. In particular, of utmost concern would be the tracking of identified or identifiable natural persons through means likely to be used by the RFID operator or any other enabled person.

RFID tags contain an amount of data related to the product, mainly in order to guarantee the origin of the product and safeguard its use through a supply chain. On this chain the product and its tag may undergo an update of the information stored on the tag. The customer – being the last receiving the particular product – will receive the product and its tag with all the information written to far; in addition, customer-specific information may be written on the tag thus possibly revealing this information to anybody who may approach the customer's purchased product and be able to read the attached tag. It is clear that the full range of privacy concerns applies at this stage.

Similarly to other emerging technologies, with the arrival of the RFID technology the lawmaker has to navigate between – on one hand - protecting the individuals, their personal data and their digital traces from being exploited too much, and on the other hand not to hinder the successful implementation of an emerging technology that could provide industry with valuable assets. In addition, it is of utmost concern to guarantee customer satisfaction from the beginning and to steer the public debate towards a positive direction.

1.1 Motivation and regulatory background

The June 2007 conference on "RFID: towards the Internet of Things" concluded with a European Policy Outlook document that lists political options and recommendations; the section on data protection and consumer awareness clearly mentions the antagonistic confrontation between data and consumer protection on one side and RFID users on the other. A general consensus had been achieved on the compatibility "with human dignity and ethical principles" and – taking into account the ubiquity – "that it is necessary to clarify the question of what must be seen as individual-related data in a world of ubiquitous information".

In May 2009 the Commission adopted a Recommendation on the data protection, privacy and security aspects of RFID-enabled applications. The RFID Recommendation gives particular attention to the concern about individual tracking and access to personal data in the retail sector (points 11-14), where it is feared that tagged items bought by individuals could be misused by

retailers or third parties for tracking or profiling purposes. It establishes the principle that tags must be deactivated at the point of sale unless the customers give their informed consent to keep tags operational. However, it allows an exception to this deactivation principle if the PIA (Privacy Impact Assessment) concludes that keeping tags operational after the point of sale does not represent a likely threat to privacy or the protection of personal data. The Article 29 Data Protection Working Party expressed its opinion to assess the risks of taking the responsibility to keep tags activated.

Point 20 of the above mentioned Recommendation requests the drafting of a "report on the implementation of [the] Recommendation, its effectiveness and its impact on operators and consumers, in particular as regards the measures recommended in points 9 to 14". The latter points refer to the use of RFID in the retail trade in which the deactivation of a RFID tag should become mandatory unless the customer – upon explicit instruction – agrees on keeping the tag activated.

In this context, DG INFSO (now: DG CNECT), in a joint effort with JRC, asked for the identification of best available techniques for deactivating tags at the point of sale in the retail sector. These techniques should obviously be privacy-, data protection-, and security-friendly, but also be economically viable to provide EU companies with a competitive advantage on the global RFID marketplace.

It was agreed that by the end of 2012 the JRC has to report to DG CNECT on deactivation techniques at the point of sale.

1.2 Definitions and limitations

(a) 'Radio frequency identification' (RFID) means 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* and all the data stored on it.

(b) 'Radio frequency tag' or 'tag' or 'RFID tag' means a device having the ability to produce a radio signal or a device which re-couples, back-scatters or reflects and modulates a carrier signal received from a *reader* or *writer*.

(c) "RFID reader/writer' or 'reader/writer' means a fixed or mobile data capture and identification device using a radio frequency electromagnetic wave or a reactive field coupling to stimulate and effect a modulated response from a *tag* or group of *tags*.

(d) "Deactivation technique", in the RFID context, means to temporarily cut off the communication (see under a.) to/from the tag so that during the cut-off no more reading can take place. Obviously the definition of 'temporarily' can mean any time range – up to infinite. Importantly, the cut-off of the tag-specific communication must be seen as a data protection-affine technique: the cut-off means non-readability of tag-specific data thus a 'deactivation technique' becomes a privacy preserving technique in the particular context.

1.3 Working methods – BATs, BREFs and scenarios

The study is supposed to set up a list of 'best available techniques (BAT's) summoned in a BREF (Best available techniques reference document). Moreover the use of scenarios has been propagated in order to get a view on all potential BAT's from various kinds of application.

In analogy to Commission Decision 2012/119/EU and similar to Commission Decision 2012/148/EU best available techniques (BAT's) are the most effective and advanced stage techniques which indicate the practical suitability for providing the basis deactivating a RFID tag at the point of sale; in particular, 'techniques' includes both the technology used and the way in which the integration and the deployment of such tags is built, operated, maintained and

generally practised. In addition, BAT's also indicate the practical suitability of particular techniques for providing in principle the basis for complying with the EU data protection framework. BAT's - in the context of RFID tag deactivation - are designed to prevent or mitigate risks on privacy, personal data and security.

'Available techniques' means those techniques developed on a scale which allows implementation in the relevant industrial sector and/or the usability at the point of sale, under economically and technically viable conditions, taking into account the costs and advantages of each technique. 'Best' means effective in achieving a high general level of protecting the customer and his privacy.

Importantly, the list of best available techniques is the result of a Member States-wide joint effort of information exchange, including industries concerned and non-governmental organisations.

The reviewing of BAT's is a continuous process, due to the nature of science, technology and privacy level considered as being protectable. Hence BAT's have to be periodically reviewed, their performance, suitability and usability regularly assessed, and, if necessary, the list of BAT's has to be updated accordingly. In addition, there should also be some mechanism that allows assuming a new and emerging technique among the ones established on the list. All these issues should best be implemented in a 'Best Available Techniques Reference Document' (BREF) steered by a stakeholder group.

'Scenario' – in the context of using RFID tags at the point of sale – means any situation in which a deactivation of a RFID tag may be considered. Hence a situation appears when a product that has a RFID tag integrated will be handed over (during a purchase process) to a customer for further use which, however, does not foresee a future commercial sale; thus the customer is the end point of the supply chain. Situations of that kind are identified according to the nature of the product and its retailer and will therefore lead to different scenarios.

1.4 Stakeholders /scenarios selection

The identification of stakeholders went in line with the recognition of scenarios, in particular use scenarios of the RFID tag technology. Basically, the following types of stakeholders have been identified:

- RFID tag **manufacturers**: Here we mean commercial companies in charge of producing hardware and software regarding RFID tags.
- **System integrator**: is a company that specializes in bringing together RFID component subsystems into a whole supply chain and ensuring that those subsystems function together.
- **Standardization organisations**: Some of such organisations have been identified which are – in the widest sense – involved in RFID tag standardization.
- **Academia**: A huge variety of scientific papers has been identified tackling the generation and use of RFID tags, in particular also including issues on privacy and data protection concerns regarding individuals carrying with them RFID-enabled products.
- **Retailers**: Supposed to be at the end of the supply chain, retailers will be in charge of applying regulations steering the correct use of RFID tags beyond the sale including their explicit deactivation at the point of sale.
- **Client**: Here we mean the person who purchases a product with a RFID tag and who is at stake when it comes to the preservation of privacy.

Regarding scenarios two typical scenarios have been identified at first: the use of RFID tags in luxury goods (luxury clothes, watches, etc.), and the developing use in automotive industry especially in car parts. Other scenario deliberately focuses on mass markets like in supermarkets. In addition, a scenario of RFID tags in textiles is of major concern because of the direct "relationship" with the person wearing the textile. Finally, a fifth scenario has been tackled regarding the use of RFID tags in books as it may reveal information on the owner's personal interests. An additional scenario that has not yet been tackled could be specified on the use of RFID tags in medical products (medicine, medical substitution parts).

1.5 How this report has been created

The JRC contribution consisted in performing a detailed study on the defining of BAT's for RFID tag deactivation at the point of sale; this study has been executed in four stages/steps:

1. **Literature review, stakeholder overview:**

   The starting point consisted in searching the literature, in particular the scientific literature, for relevant publications in the field of RFID tags, possible deactivation techniques and aspects of privacy and data protecting measures.

   The literature review consisted also in identifying relevant stakeholders in that field.

2. **Analysis and listing of available techniques:**

   Focusing on temporary deactivation of active RFID tags implies questions on the duration of the deactivation, expiry of this period, possible reactivation of the tag, and implications on the physical status of the tag itself.

   The study deliberately excluded issues regarding the expiry of the deactivation as well as the possible reactivation of a deactivated RFID tag (except for the case that an attacker may try to reactivate it).

   An analysis of the available techniques revealed a basic distinction into a (physical) destruction of the RFID or not. The latter classification has been further divided into (a) techniques that do not destroy the tag itself but may gradually reduce the communication skills of that tag so that privacy preserving issues may be fulfilled, and (b) techniques based on all other kind of more or less traditional measures.

3. **Workshop with stakeholders (15 – 16 October 2012, Ispra), bilateral interviews:**

   It was part of the agreement with DG CNECT to organize a workshop inviting stakeholders in order to

   1. Make an inventory of available RFID deactivation techniques,
   2. Make an inventory of challenges in respect to data protection, security and economic viability,
   3. Define relevant scenarios of the retail sector,
   4. Rank techniques towards best available ones.

   This workshop had to be canceled and as compensation a variety of bilateral interviews have taken place.

4. **Questionnaire to selected stakeholders:**

   A questionnaire has been developed regarding a variety of points that should clarify important issues in the context of establishing the list of BAT's.

2. RFID Tags, Privacy Issues and Related Countermeasures

In this section we present RFID tags, some related potential privacy threats and solutions to mitigate and prevent them.

2.1. RFID Tags

An RFID tag is basically a device composed of a small *chip* connected to a *coil*. The chip is essentially a state machine with a memory, providing limited storage and computation capabilities. The coil, that is typically referred to as the *tag antenna*, is used to power the chip and as communication interface. In particular, for the communication with such devices, an RFID tag *reader* has to be used (Figure 1). The reader emits a radio frequency (RF) field that by induction through the coil powers the chip. At the same time the reader properly modulates the field to code commands sent to the chip, which in turn replies to the reader modulating the same field, so establishing a bi-directional communication. For a correct read-tag interaction the tag has to be dipped into the reader field area so as to receive enough power for its activation. The working *range*, namely the minimum distance required for a tag from a reader to be activated, depends on the specific adopted RFID technology and its properties, and different solutions are available on the market.

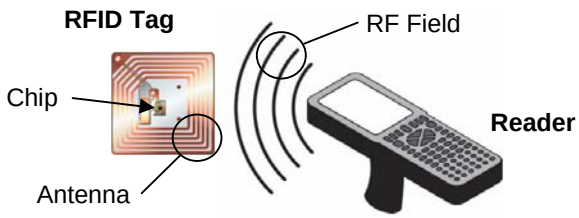

Figure 1. RFID tag and reader

The typical purpose of an RFID tag is to memorize data and release them when queried by a non-contact reader. According to this peculiarity their main application is item labelling. RFID tags can be stuck on or embedded into items to track their position, reading the tags at different places, and to easily get information about them storing specific item-data in each applied tag. The information gathered from a tag can also be put in relation with additional item data stored in a back-end system (Figure 2). Concerning this, we remark how the focus of this report is on item labelling and so on RFID tags and not on contactless smart cards, which are similar devices that adopt an analogous communication mechanism, but that are featured by different capabilities and are suitable for other kind of applications [1][2].

2.1.1. Tag Data

In the context of item labelling RFID tags are typically designed to store some of the following data in their memory:

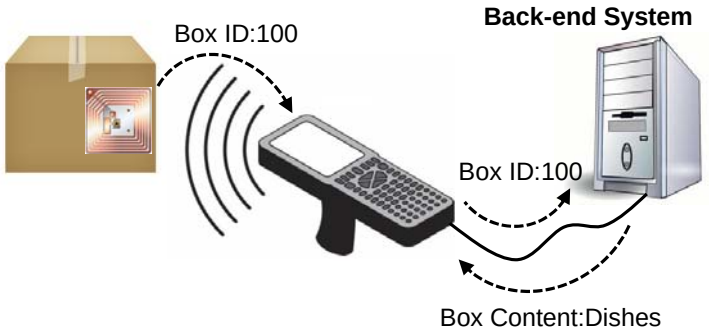

Figure 2. Typical scheme for RFID tags used for item labeling

- Unique Item Identifier (UII): a number assigned to a specific item and that is used to uniquely identify it (in Fig.2 it would be the ID returned by the tag to the reader). This field can be formatted according to standards making this value unique in the world for all time (i.e., EPC codes [3]). It is typically used to access a data base and get further information about the tagged item;
- Tag Identifier (TID): a number uniquely identifying an RFID tag itself, as physical device, and which is put in the tag memory by the tag manufacturer at the time of the device manufacturing. This field is typically write-locked, so neither it can be manipulated nor erased, and the main purpose is to make tag duplication harder when such devices are embedded in items requiring originality certifications [4];
- User data: generic data regarding the labelled item and put on the tag memory by the final user according to his application requirements.

Such information is typically accessed using an RFID reader addressing the different tags memory locations. We point out that, in principle, a reader could be also allowed to write data on a tag, depending on the adopted tag technology and the defined application.

2.1.2. Communication Architecture

The tag-reader interaction is achieved according to the communication architecture shown in Figure 3. It is basically a stack featured by three layers that we briefly explain below:

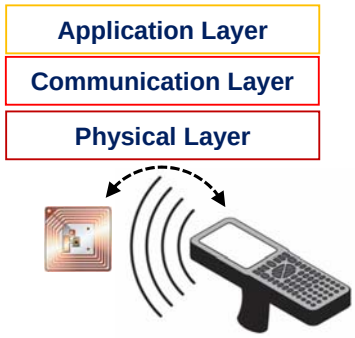

Figure 3. Tag-Reader communication architecture

- Physical layer: it is the basic brick to implement the tag-reader communication, defining a way to exchange data between the two parties. At this layer it is specified how the RF field used for the communication has to be modulated by the reader and by the tag to encode information (i.e., data bits) sent to the counter-party;
- Communication layer: this layer specifies how the transmitted data using the Physical layer have to be organized in terms of time and format. In particular it defines how the data are bundled before they are sent to the counter-party, so that the recipient of the communication can correctly interpret them (e.g., fields and format featuring commands sent by the reader to the tag, returned tag data format), and the timing of the messaging to establish an ordered interaction. In addition, another important communication aspect is typically defined at this level, the *singulation* protocol. When different tags are in the RF field area of a reader, it needs a way to discriminate these tags in order to establish single interactions with each of them. This is achieved through the singulation protocol, which is typically run at the time the reader starts a new communication session switching its RF field on. During this initial phase each tag identifies itself to the reader, for instance communicating an identifier (Figure 4), that will be then used by the reader as a tag address to individually contact them;
- Application layer: at this level, typically, the tag content is defined together with relative encoding, that is returned after a reader inquiry relying on the infrastructure defined by the two layers below. In this layer other application operations could be also defined (e.g., control of the tag content access by presentation of credential, authentication, update of tag data).

For these layers different defined standards exist, each one featured by its own characteristics (e.g., working range). We will cite some of them pertaining to this report in the next section.

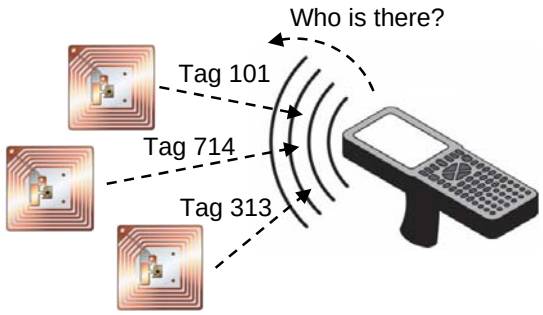

Figure 4. A tag singulation example

2.1.3. Additional Remarks

In the end we remark some RFID tag peculiar properties that are relevant in the context of this report:

- no switching-off: RFID tags cannot be switched-off as their powering is based on the field emitted by an RFID reader, so whenever a tag is placed in a reader field it is activated and available;
- activity without explicit control: RFID tags automatically reply to reader interactions without explicit control of the tag owner, so RFID tags can operate without their owner's consent;

- wireless communication: it is easy to establish a communication with an RFID tag and there is not any visual confirmation of a tag-reader interaction (i.e., not wires or manual operations required), so it is possible to interact with an RFID tag without being detected.

According to such properties and the typical tag content some privacy issues can arise and we cope with this aspect in the following section.

2.2. Privacy Threats

We present now the context in which possible RFID privacy threats are considered and provide some related technical details.

2.2.1. Context

Our reference scenario is the production and distribution of goods. In order to optimize the management of produced goods along the whole supply chain up to the final consumers, RFID tags can be applied on the goods to enhance their traceability and information gathering. We focus in particular on the *retail sector*, meaning the end of the supply chain is represented by shops with single products sold to individual citizens. In such a case, the delivered products, after the *point of sale (POS)*, could still be equipped with working RFID tags (Figure 5).

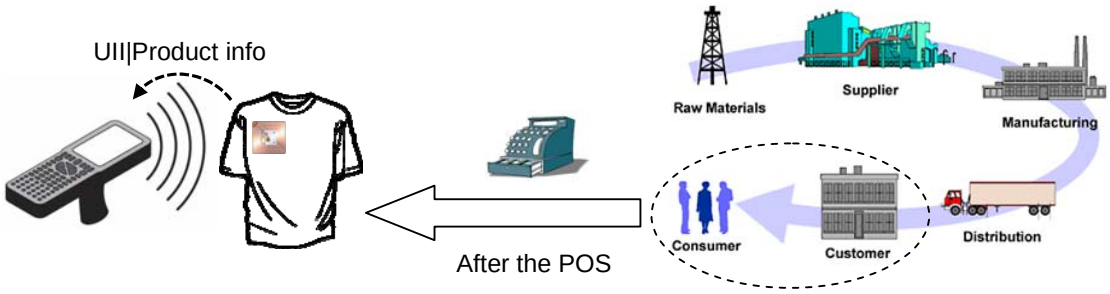

Figure 5. The reference scenario: supply chain and working RFID tags after the point of sale

We focus on this scenario as the presence of RFID tags in products sold to consumers is explicitly addressed in the European Commission Recommendation of 12/05/2009 on the implementation of privacy and data protection principles in applications supported by RFID [5]:

> *"In the retail trade sector, an assessment of the privacy and data protection impacts of products containing tags which are sold to consumers should provide the necessary information to determine whether there is a likely threat to privacy or the protection of personal data."*

With regard to the possible privacy threats in such a context, it is important to point out that the RFID tags typically used for item labelling are featured by a working range of 1-4m, according to the standard the tag is compliant with (some of the typical reference standards in item labelling are the ISO/IEC 15693 [7], ISO/IEC 18000-3 [8], ISO/IEC 18000-61:64 [9:12]). This remarks how the interaction with such a tag can be achieved from a far position. Then considering the possible information stored in the chip (unique identifier, product information, see Section 2.1.1) and the peculiar characteristics of an RFID tag (always on, "hidden" interaction thanks to the wireless communication and interaction without explicit control, see Section 2.1.3), the following threats could affect the final consumer in case the tags in the purchased products are still working after the point of sale (Figure 6):

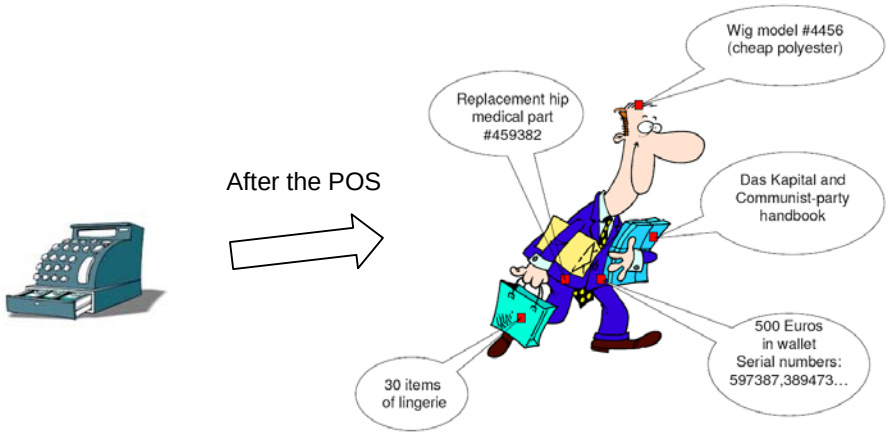

Figure 6. Potential RFID tag-related threats: information leakage and traceability possibility [6]

- Position Traceability: a unique identifier could be stored in the tag (i.e., the UII); if it is possible to associate such an identifier to a specific person, it would also be possible to track the person's position reading the tag at different locations (e.g., this could be the case of a person wearing a T-shirt with a tag in it);
- Information Leakage: according to the kind of data stored in the tags it could be possible to gather some information about the person's belongings, simply reading out the content of the tags applied to/embedded into the items he/she brings with himself/herself. We point out that even in the case only an UII is stored on the tag, that by itself could represent a meaningless value, solutions for retrieving product information from the relative UII may be made available, for instance through online services (e.g., [13]). In addition, due to the over-the-air nature of the communication, it could also be possible to improperly recover information about the person's belongings eavesdropping the messages exchanged between a reader and a tag (e.g., if tags and reader interact at a POS in a shop, it could be possible to eavesdrop their messages out of such shop knowing in advance the items bought by the consumers that are going out of it). Concerning this we point out that the messages from readers towards tags are featured with a greater RF power and are consequently easier to eavesdrop compared to the messages sent by the tag itself [14][15]. So care should be taken in particular to the sensitivity of data transmitted by the reader.

Thus, in case no countermeasures are taken, RFID tags used in the retail sector can leave open privacy threats for the final consumers.

2.2.2. Threats in the Tag Communication Architecture

We summarize the different ways by which the above-mentioned privacy threats can creep in the tag-reader communication architecture. According to the following Figure 7:

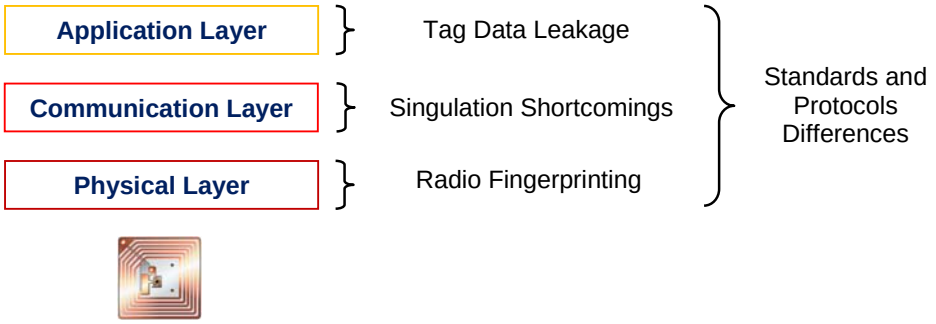

Figure 7. Privacy threats in the Tag-Reader communication architecture

- Some studies have been conducted to evaluate the possibility to discern different tags according to their peculiar characteristics in the transmitted signal, so focusing on the Physical layer [16][17]. The signal transmitted by the tag is analyzed through signal processing procedures and specific features of such signal are highlighted. The extracted features differ among different physical tags and can be used as radio fingerprints to discern them. Such an analysis is not easy to apply in practice, but in case of further developments it would open new traceability scenarios, as it would be possible track a tag reading its signal at different locations and then extracting its radio fingerprints;
- According to the singulation protocol adopted at the Communication layer, privacy issues can arise. During such a protocol the tags identify themselves towards a reader, but they have to do this in a randomized way for each interaction session. Indeed, in case they use for instance a fixed identifier during each singulation with a reader (e.g., like the binary-tree collision arbitration mechanism of ISO/IEC 18000-62 [10]), such an identifier could be easily used for tracking purposes. This concern is not only relative to fixed identifiers, but also to any form of determinism linked to a specific tag that can be exploited to discern it among others (e.g., selection of the same time slot for each communication session in case of time-slotted communication with the readers [18]). In addition, if the information transmitted relaying on the Communication layer is not properly protected, due to the over-the-air nature of the communication, data interception could be possible by eavesdropping the data bundle transmitted at this level;
- The privacy risk associated to a tag also depends on the kind of data that are stored and accessible in the chip's memory for the relative application purposes. As already mentioned unique identifiers and information regarding the tagged item can raise privacy issues. In addition, not only item-related data, but also the presence of a TID in the tag memory could be misused for tracking purposes, as it represents a number uniquely identifying the physical device. We also remark that if at the Application layer operations to write in the chip's memory are designed and allowed, a malicious subject could even write for instance a his/her own identifier in the tag for tracking purposes;
- For a tag implementation different standards and solutions are available, defining for instance the signal characteristics at the physical layer, communication rules at the communication layer, data format in the chip's memory and sequence of operations for accessing the tag content at the application layer. If a person brings with him/her a set of tagged products from different retailers who adopt different tag implementations, it would be possible to design a person profile based on a tag constellation [18][19] (e.g., the target person is featured by three tags that work according to three different

frequencies at their physical layer or that are featured by three different methods to get access to the internal data). Tag constellations could be used for tracking purposes.

So countermeasures should be foreseen at each level. The tracking based on physical RF fingerprinting is currently hard to apply in practice and the use of a single uniform standard defining aspects of the physical and communication layers is not achievable, as the different standards are designed to satisfy different application requirements and are applied accordingly. That being so, the main efforts to develop RFID tag privacy preserving techniques have been driven to tackle the issues emerging from the communication and application layers.

2.3. Privacy Threats Countermeasures

In this section we present a set of solutions to prevent or at least mitigate the different privacy threats featuring RFID tags.

2.3.1. Context

The use of countermeasures to prevent privacy issues deriving from the use of RFID tags in the retail sector is explicitly recommended in the European Commission Recommendation of 12/05/2009 [5] through the following two articles:

> *"RFID applications used in the retail trade*
>
> *11. Retailers should deactivate or remove at the point of sale tags used in their application unless consumers, after being informed of the policy referred to in point 7, give their consent to keep tags operational. Deactivation of the tags should be understood as any process that stops those interactions of a tag with its environment which do not require the active involvement of the consumer. Deactivation or removal of tags by the retailer should be done immediately and free-of-charge for the consumer. Consumers should be able to verify that the deactivation or removal is effective.*
>
> *12. Point 11 should not apply if the privacy and data protection impact assessment 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 the protection of personal data. Nevertheless, retailers should make available free-of-charge an easy means to, immediately or at a later stage, deactivate or remove these tags."*

Thus, according to these two articles, two related groups of possible countermeasures can be identified and applied at the point of sale: privacy preserving techniques that keep a tag operating after the point of sale and techniques that make a tag definitely inoperative after the point of sale, or anyway not linked anymore with the original item it was attached to or embedded into. Thereafter we have organized our reviewed list of privacy preserving techniques accordingly, in two groups, presented in Section 2.3.3 and Section 2.3.4.

We also remark: as RFID tags in the retail sector are typically featured with low computation and storage capabilities, the idea is to have cheap devices that should be applied to many products massively manufactured by companies. This is crucial to keep the tag cost negligible compared to that of the tagged products, in particular when the value of such goods is low. Concerning this, RFID tags are also typically not tamper-proof devices: the chip can be dismantled getting physical access to the internal memory and thereby to the relative content. Such constraints reduce the number and the kind of privacy preserving solutions implementable

on such devices. The countermeasures that have been proposed, and that we have reviewed, typically try to take into consideration such constraints. According to the specific application scenarios more expensive and so more powerful tags could be developed, opening the possibility of more complex and efficient privacy preserving techniques.

The European Parliament states in a study [56] that electronic labelling, or RFID tags in textiles, is still in its infancy. Also, while it is clear that electronic labelling will benefit industry, the benefits for consumers are still in the infancy stage. The main concern related to consumer's use of RFID is the privacy issue, which must be solved before introducing RFID chips to consumers.

2.3.2. Available Techniques

This section is for the privacy preserving techniques that are achievable, and so available, according to the current technologies.

2.3.2.1. Tags Operating after the Point of Sale

Here there are the privacy preserving solutions that allow a tag to be still operative after the point of sale, meaning that is possible to active it and interact with it through an RFID reader but the related privacy risk is nullified or at least mitigated. This kind of solutions can be useful in case the retailer or the consumer might use the tag for post-sale activities (e.g., management of returned items, product warranty).

Basic Countermeasures

When a tag is kept operative after the point of sale, along with a privacy preserving technique an additional set of basic countermeasures could be necessary, otherwise there could be the risk to invalidate the effectiveness the adopted technique. Thus in general, upon these countermeasures, the selected privacy preserving solution is applied. In particular:

- It is fundamental to avoid any possible traceability relying on the singulation protocol, so any form of fixed identification or determinism should be avoided a this level, typically adopting randomized algorithms that rely on cryptographically sound pseudorandom number generators installed on the tags, allowing for instance the presentation of a random number as session identifier at each interaction towards a reader;
- Writing on the tag's memory should not be allowed or at least regulated through the use of a password (for instance using write-locking procedures [11]);
- It is advisable to encrypt at least the communication from the reader towards the tag (e.g., cover-coding of [11]) in case the transmitted, and eaves droppable, information could be used to somehow profile a person.

Tag Data Modification

The idea is to reduce the traceability of a tag or the meaning and the amount of the data stored in it. For instance, if the tag data is organized in sub-fields, like a unique item identifier and some item information, the field uniquely identifying the item could be erased [20] (Figure 8). In this way the tracking possibility is mitigated, even if tracking based on tag constellations may still be possible. As different approach, according to the application scenario, the tag content could be re-written with consumer specific data allowing post-sale use of the tag in a private scenario [21] (e.g., new unique identifier for personal item management), in this case breaking any links with the original stored information related to the item. For instance, in this case the possibility to retrieve information about the item linking its tag content with an online database would be prevented, even if its traceability remains possible. Thus, after the singulation procedure, when

the tag is addressed by the reader, it returns a reduced/modified set of data compared to its original content used for the supply chain management. Note that attention should be paid not only on the item data stored in the tag like the UII, but also on other potential data exploitable for profiling (e.g., the TID).

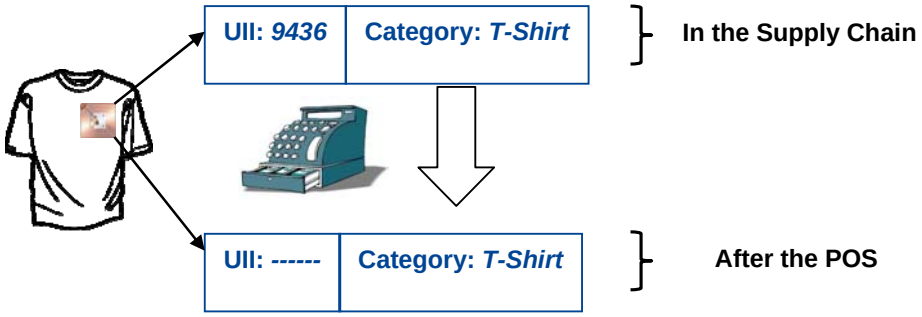

Figure 8. Example of tag data modification at the POS for reducing the tag traceability

A similar solution, but not entailing any tag data modification, would be the use of multiple tags, with for instance one tag on the case containing the items and one tag for each item in the case [21]. The one on the case could store some item information (e.g., category), whereas the ones on the items could contain their relative unique identifiers. When the items are taken away from the case, the full information is broken.

In case the whole tag content could be useful for post-sale activities, rather than erasing part of the information, the data stored in its memory could be partially and temporarily hidden (for instance at the point of sale switching from a public to a private profile [30]) and re-enabled when required.

Password-Regulated Access

The tag content access is regulated through a secret password stored in its memory (Figure 9). After the singulation protocol the reader can address the tag as usual, but before requesting the relative data it presents a secret password. The tag compares the received password with the one internally stored in its memory and in case of matching allows the reader to access the internal data, otherwise denies the access [11]. It is recommended to encrypt the forward channel, from the reader towards the tag, mitigating the possibility to eavesdrop the wirelessly transmitted password (see cover-coding in [11]).

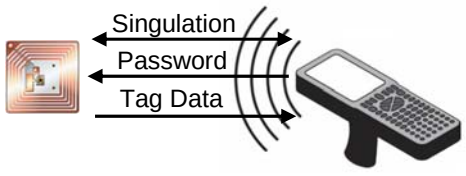

Figure 9. Password-protected tag content access

This solution is anyway featured by password management issues. Indeed, if for instance a single password is adopted to regulate the access to all the tags of a retailer, in case such password is disclosed, the whole system security is demolished. Concerning this, we remind that RFID tags

used in the retail sector are typically not tamper-proof devices, so an attacker who comes into possession of one tag could dismantle it and recover the internally stored shared password. On the other hand, if a single password per each tag is used, it is anyway necessary that each tag uniquely identifies itself before the password presentation (e.g., with a fixed unique identifier during the singulation protocol), so that reader-side it is possible to retrieve the right associated password (e.g., accessing a data base storing identifier-associated password entries). In this second case we are obviously leaving room for tracking possibilities.

In addition we point out the following study [22], where the authors adopt a side-channel analysis to start recovering some information about the password stored in a tag. In particular, as tags are powered using the reader RF field, it seems possible to analyze reader-side the tag absorbed energy and correlate it with the tag internal password, in particular acting in a complete remote way.

Reduced Working Range

The aim is to reduce the tag communication range. There are basically two approaches: physically acting on the tag structure or sending a command to the device.

In the former approach a portion of the tag antenna is physically removed (Figure 10) so that the tag can still operate but only at short ranges from the reader (e.g., working range reduced from 3m to <10cm) [23][24]. In this way it is harder to activate the tag, interact with it and get access to its content.

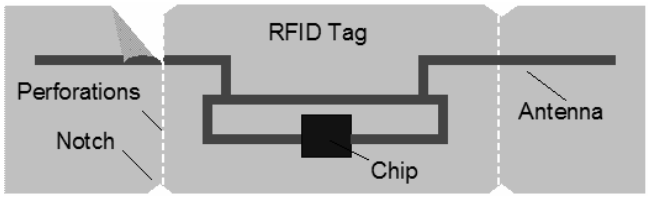

Figure 10. Tag with partial antenna removal (figure credit: [23])

For the latter approach, the tag has to be explicitly designed with an onboard mechanism to restrict its communication capability, so as to reduce the minimal distance useful for an interaction with it, and such a mechanism may be activated through a command. A possibility is represented by an onboard solution to evaluate the reader RF field strength and only if a threshold is exceeded the internal content is released [30], considering that the higher the RF power at the tag antenna, the closer the reader is.

The basic idea behind this kind of solution is that a reader is close to the tag only when the user is physically giving authorization for its readout.

2.3.2.2. Tags Not Operating after the Point of Sale

With the following techniques a tag is made definitely inoperative after the point of sale, or it is not linked anymore with the original item it was attached to or embedded into.

Kill Command

It is a password-regulated command that can be sent to a tag (Figure 11): the tag compares the password received in the kill command with a password internally stored in its memory and in

case of matching the tag is made unresponsive forever, so not reactive to any reader interactions, otherwise it keeps working normally [11].

Figure 11. Kill command applied at the POS

Tag or Antenna Removal

The tag is physically removed from the item. The tag is still working but there are no more any tags on the item to interact with, so the item-tag link is broken.

Another possibility is the complete removal of the tag's antenna, so that it is no longer possible to interact with the chip, as powering and communication with it are impaired. As further development, the authors of [25] hypothesize the development of a tag with the possibility to re-apply an antenna at a later time (e.g., antenna-stickers), so re-enabling the communication with the chip when and if needed. If such a solution would be developed, we could insert it in the tag operating after the point of sale solution list.

Both for antenna and full tag removal, a particular design of the device packaging would be typically required, allowing its removal from the applied item (e.g., notched line, sticky tags).

Tag or Antenna Destruction

This solution is similar to the previous one, with the difference that a physical/mechanical action on the RFID device to alter its structure and compromise its functionality is required, maybe using a tool. For instance a pair of scissors could be used to cut the tag chip or only the tag antenna. Care should be taken during this operation, as for instance a partial cut of the antenna could keep the tag working, even if at shorter ranges, or for the chip cutting a precise operation right on it would be required. That being so, this solution differs from the previous one as no particular tag packing design would be typically required, but specific skills for the operator could be needed. As an advantage, this trivial solution could be applied in all those circumstances where an explicit tag deactivation solution was not foreseen.

2.3.2.3. Putting it all together

In the figure below (Figure 12) we summarize the presented privacy preserving techniques suggesting also some possible combinations.

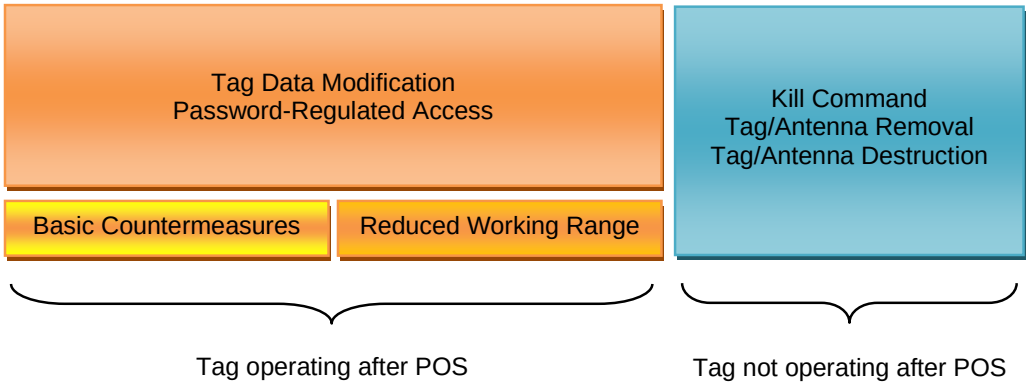

Figure 12. RFID tag privacy preserving solution summary

In case of tags that require keeping working after the point of sale, it is possible to adopt the basic countermeasures upon which the tag released data is reduced/modified or the relative access is regulated through a password. As an alternative, the tag content could be kept as is also after the point of sale, but just reducing the device working range. Apart from these two possibilities, further combinations could be also realized depending on the specific application scenario. For instance the use of a reduced working range along with a password-regulated access with a specific password for each tag would allow revealing the fixed tag identifier, fundamental for the use of the correct password, only at short distances. The techniques for tags not operating after the point of sale are instead in mutual exclusion.

2.3.3. Other Techniques

Many other privacy preserving solutions have been proposed in the literature. They are, in general, works proposed in academic studies that have not found a practical application so far, typically due to limits of the currently available technology that may impair any real implementation. For the sake of completeness we give a brief overview of these other techniques:

- Tag press-to-activate: the tag does not communicate by default. The tag replies to a reader inquiry only if it is explicitly activated by the user at the time of the readout pressing a button on the device [27] or through a touch interface (e.g., a capacity touch interface [26]). Such a human interface has to be designed and implemented on the tag;
- Secret handshaking activation: with this solution the tag also does not communicate by default. The tag is equipped with some additional sensors, typically MEMS (Micro Electro-Mechanical Systems), and incorporates a gesture recognition algorithm, so that when it is powered by a reader field it is able to detect if it is undergoing some specific movements in the space. The tag replies to a reader inquiry only if it is explicitly "activated" by the user at the time of the readout through a specific gesture [28];
- Blocker tag: a Blocker tag is a special tag that when is in proximity of other normal tags impairs their readout by a reader [29]. A user could carry a Blocker tag so that the readout of the tags present in its local environment is blocked. The solution could be refined so that a Blocker tag hides only a subset of tags, as for instance only those tags featured by an UII in a specific range called privacy zones. A tag UII could be re-written to enter/exit a privacy zone, so as to block or not the tag readout in presence of Blocker tags. The Blocker tag solution works at the singulation protocol level and has been in

particular designed for a specific singulation protocol [10], but the authors state that it can be extended to other ones. On the other hand, such a tag could be used maliciously for denial of service attacks, easily impairing tag-related activities;

- Cryptography-based solutions: many cryptographic solutions have been designed so far, their main aim is basically to randomize the tag output over time so as to prevent any privacy threats (i.e., no static identifiers and no explicit item information). Many of these solutions have been designed to require the execution of lightweight crypto-algorithms on tag-side, as such devices typically present low computation capabilities. Such solutions have encountered feasibility problems so far, as it is even problematic for the implementation of lightweight algorithms on these low cost and poor resourced devices. In addition, some of the proposed solutions do not scale well when the number of tags increases in the system, as huge computations become necessary reader-side. A proposed solution relies on pseudonyms [31]. The tag does not store a unique item identifier but a set of different pseudonyms, replying to each reader inquiry with a different pseudonym. On the reader-side the pseudonym set of each tag is stored, so that it is possible to discriminate the different tags of the system. In order to avoid frequent replies with the same pseudonym by a tag, the pseudonyms in the tag set are returned in a cyclic way, and as further countermeasure a mutual authentication mechanism between reader and tag is available; this allows, at each authenticated read out, the reader to replace a tag pseudonym with a new one, thus renewing the pseudonym set.

  Another proposal is based on cryptographic hash functions [32]. The tag stores an internal state value. At each reader inquiry the internal state is given as input to a hash function whose output is returned to the reader, while the internal state is updated to a new value used for the next readout. The reader system has to be synchronized with all its associated tags storing their current internal state, so that when a tag replies, the returned value is compared with the hash of all stored states thus identifying the tag and updating the relative stored state. A different possible scheme resembles a private authentication [33]. At each read out the tag randomizes its identifier through random generated values and secures the resultant value through cryptographic operations based on a private key shared with the reader system. Each tag features its own private key that is stored and associated with the tag identifier on the reader-side. When the tag generated values are sent to the reader system, it iterates a set of operations on the received data, trying all stored tag keys, thus obtaining in the end the original tag identifier. Many other schemes have been proposed to periodically re-encrypt the data stored in the tag. For instance the tag data could be re-encrypted at each valid readout by the reader system [34][35][36]. As further development different readers could be deployed in several places and, when a tag comes into their proximity, the relative content is re-encrypted [37][38].

In the end we point out that some RFID tag-related ISO standards and international specifications are currently under revision for the inclusion of new privacy and security functionalities.

3. Scenarios at the point of sale (POS)

The application and use of RFID in the supply chain and its presence in goods at the moment of purchase is relatively complex and versatile. To be able to discuss and compare the RFID applications it was decided to concentrate on particular representative scenarios. These scenarios represent the business process, which is seen as a collection of related, structured activities or tasks in the retail sector for a particular customer. The RFID is very useful in tracking products and apparel products at every stage of their production and existence. The customer in this case

is the one purchasing a RFID labelled product. Figure 13 shows the abstract process at the POS related to the RFID and its deactivation.

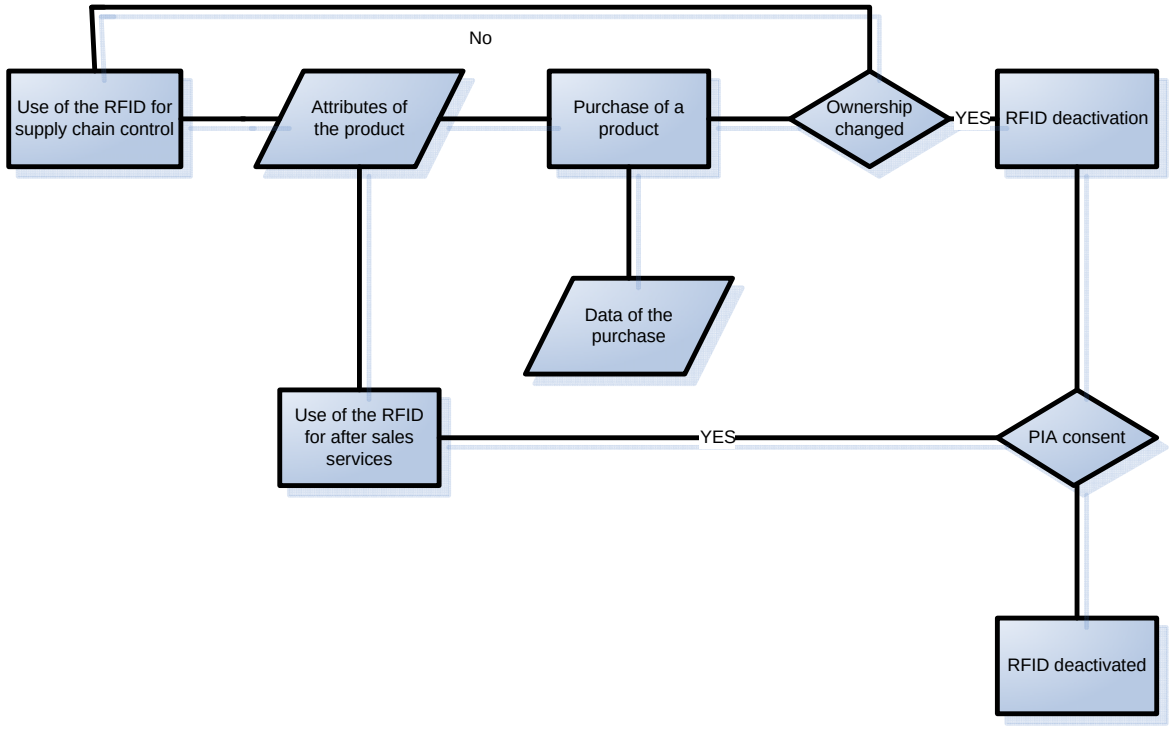

Figure 13. Flowchart of the process at the POS relevant for the RFID

The following five scenarios are representing a wide range of retail activities and can be considered due to their specific aims and attributes very relevant to discuss the deactivation of the RFID:

Textile: large diffusion of consumer textile goods, with issues regarding identification, tracking and location. Clients may wish to return the goods.

Books: Bookshop environment, with the possible extension of having book loans in libraries. The book content may have a specific significance regarding religion, personal lifestyle preferences, or medical interest.

Large distribution: low nominal cost goods. The solution for deactivation needs to be low cost as well, and the speed at the point of sale is an economic parameter.

Luxury goods: deactivation solution may be expensive, and speed at the point of sale is less an issue, but the deactivation is challenging, as security, fraud, theft, tracking and product authentication are at stake.

Automotive industry (cars): supply-chain management, identification of spare parts when replacement is needed and managing the recycling at the "end of life" push for massive tagging. As a car may therefore host 'hundreds' of tags, deactivation or any type of anonymisation provisions are necessary (tracking and location related issues).

3.1. Textile

This classical but specific scenario regards large diffusion consumer textile goods, with the particularity that the owner potentially wears the textile. This opens a collection of issues regarding identification, tracking and location. It is also a good one client may wish to resituate. Retailers such as Decathlon, Walmart, Gerry Weber, JCPenney, Marks & Spencer, Metro and Macy's have all rolled out extensive RFID item-level tagging, where savings are being tracked principally in supply chain precision and back room operations.

In 2010 the European Parliament discussed in [56] the use as RFID for labelling textile as one of the labelling options. The debate on textile labelling was spurred by a proposal for a Regulation on textile names and related labelling of textile products. The study of the European Parliament investigates whether other textile labelling requirements could be brought up in EU legislation, including care instructions, chemical substances in textiles, electronic labelling (RFID), multi-lingual, country of origin, ecological, and size labelling.

According to [55] RFID is revolutionising all aspects of fashion logistics, from manufacturing through distribution and retail, based on simple and effective item level identification of textiles and garment. The proven benefits of RFID have convinced global leaders like DHL Fashion and Marks & Spencer to adopt this technology to improve all aspects of fashion logistics. The impact on the business sale cycle was nothing short of remarkable – time for stock-taking was reduced more than ten-fold, the accuracy of on-shelve replenishment improved beyond recognition, and retail sales at stores employing RFID increased by more than 10% compared to other stores.

The BRIDGE project is highlighted in [56] as it has tested the most promising ways of introducing RFID in the textile sector: to manage the supply chain and to some extent to improve the information to consumers and the shopping experience. The BRIDGE project was a 3-year FP6 project that began in 2006. Textiles were one area of the project that applied RFID in pilot projects and experience in real-life environment, as well as developed a business case for RFID. In order to receive representative results, three different business models were used for the pilot projects: a department store, a hypermarket, and a SME supplier. Retail was found to benefit the most from RFID technology, particularly in inventory management.

RFIDS are easily affixed onto textile products using a standard sewing process, enabling reading distances over 3 meters using for example TAGSYS UHF reading Stations. LinTRAK for example designed tags for flat linen and uniform identification; it can be sewed along the edge of the item or incorporated in the hem. LinTRAK withstands heat-sealing processes and can be attached to the textile article using a standard adhesive patch. New applications for the technology are being developed all the time, one of the latest being a "truly textile" RFID label for the fashion industry. The all-in-one solution has been developed by Swiss-based TexTrace AG, a subsidiary of ribbon and narrow fabric specialist Jakob Müller AG, which has launched a sewn-on brand label into which a special flexible high-performance antenna yarn is interwoven and which is assembled with an encapsulated RFID chip - making it indistinguishable from a normal fashion label.

Figure 14. Concrete RFID application in the textile field with suggested deactivation technique.

RFID (in textile industry) is proving to be a late bloomer. While it has not yet seen the explosive growth some were predicting a few years ago, the technology continues on a slow and steady curve upwards, with 2.88bn tags sold in 2011 versus 2.31bn in 2010 (a 24.6% increase), according to UK-based RFID analyst IDTechEx.

After an extensive pilot test, Gerry Weber initiated a groundbreaking project for the entire supply chain in 2009. Within the scope of this project, RFID has been deployed not only to optimise the processes of logistics and retail, but also to function as a new form of electronic article surveillance. Since January 2011, we have equipped more than 26 million of our annually produced articles of clothing with RFID technology. Together with renowned partners including Deutsche Telekom, Deutsche Post DHL, the label manufacturer Avery Dennison and logistics providers Meyer&Meyer and Fiege, this project has not only resonated very positively within the industry, but also has elevated the Gerry Weber company to the role of pioneer in the field of RFID technology in retail.

3.2. Supermarkets

Supermarket of today and the future are seen as wireless express checkout and smart shelves that alert staff to expired cream cheese. They are selling a number of products in average of low nominal cost. The solution for deactivation needs to be low cost as well, and the speed at the point of sale is an important economic parameter. At least that was the vision the German retail chain Metro AG promoting with stores showcases using RFID technology. The use of wireless equipment, in combination with older technology such as bar codes, is often an attempt to find out what will cut costs and attract customers. "We are just at the beginning of the technological modernization of retailing," says Metro CEO Hans-Joachim Koerber about 10 years ago. Key feature at Metro AG were smart RFID chips that broadcast data for several centimetres, enabling receiver-equipped smart shelves or handheld scanners to track what's in the store and what goes out of it.

In that situation, low nominal cost goods (mean, as some may be expensive) represent a challenge. The solution for deactivation needs to be low cost as well, and the speed at the point of sale is an economic parameter.

RFIDs are used on top of the labelling good for different purposes in a supermarket. ALDI and Lidl are both using for example active tags from Albis Technologies to ensure only authorized personnel enter their warehouses; Lidl is also using the technology for its freezers.

3.3. Books

This specific scenario regards book selling in book shops. The nature of a paper book is specific and the scenario can profit from the tagging of books in libraries. The book has a specific significance to the meaning of its content in respect to the buyer. This counts for the lifetime of the book as buying, owning and carrying it in certain situations can profile the one having the book in respect to:

- Religion
- Personal preferences
- Medical literature in respect to disease.

According to [65] RFID technology is seen as a radical innovation, or even as the successor of barcode, that offers new opportunities for bookstore RFID in bookstores retailers. RFID also entails many questions and uncertainties about the maturity of the technology and the fit within the independent bookstore. There have been many pilot projects setup concerning RFID applications in retail. The results of the projects often look promising but are very dependent of the type and level of RFID technology applied. In 2007, one specific RFID project became very famous. Dutch book retailer BGN rolled out RFID in their new Selexyz bookstore. BGN took RFID beyond the pilot stage and adopted the technology on item level, representing the whole store inventory. At the end of 2007 they announced to roll-out RFID in all of their branches in the next years.

In our days book tagging with RFID is also used in libraries. Though this use case represents a different scenario from selling books at the POS in book shops, it is referenced here as it delivers and contributes experience and knowledge. RFID is the latest technology to be used in library theft detection systems and the ability to scan books on the shelves without tipping them out or removing them for inventory purposes. RFID-based systems move beyond security to become tracking systems that combine security with more efficient tracking of materials throughout the library, including easier and faster charge and discharge, inventorying, and materials handling.

RFID is a combination of radio-frequency-based technology and microchip technology. Another application of RFID technology is automated materials handling. This includes conveyer and sorting systems that can move library materials and sort them by category into separate bins or onto separate carts. This significantly reduces the amount of staff time required to ready materials for re-shelving. RFID tags last long. Vendors claim a minimum of 100,000 transactions before a tag may need to be replaced [57].

3.4. Luxury goods

The operational scenario of the luxury goods has specific features in comparison to other scenarios, because of the typically high price of the goods. In particular the tracking of a luxury or high value good carried by a customer can be interpreted as a sign that the customer has high-income or considerable economic assets, which can increase the possibility of theft. For example, a criminal can try to detect all the persons carrying valuable clothes or bags at the entrance of an apartment block to identify potential targets for burglary attempts.

In this context, the tracking of luxury goods and the association to their owner can represent a privacy breach because it can indicate the economic or social status of a person or his/her preferences.

Beyond specific privacy concerns, the presence of RFID on luxury goods carried by an owner or located in the property of the owner (e.g., in a house or in a car) can also introduce security and safety concerns, because a criminal can exploit this knowledge to carry out a theft. This is a threat, which is not so relevant without RFID technology, because the luxury good can be hidden from view, while the electromagnetic field of a RFID can be detected from outside the property (e.g., outside a car). Note that the limited range of RFID reader can be easily increased by using directional antennas or amplifiers, which can be configured and deployed with simple technical knowledge as described in [40]. RFID readers can be inserted in mobile phones and can be purchased at low cost.

As described in [41], manufacturers of luxury goods have started to deploy RFID labels on their products, so the threats described above can become more likely in the near future. The solution described in [41] does also include a kill command to protect the privacy of the customer.

On the other side of the coin, the application of RFID technology to the luxury market can defend consumers from frauds and counterfeit goods and protect luxury goods manufacturers from economical damage. The deployment of RFID tags in many types of luxury goods is quite easy as it can be embedded in the garments or the labels and the cost of the RFID tag is adequately justified by the price of the luxury good.

The FP7 BRIDGE project has investigated the application of RFID tags in the luxury market to address the problem of counterfeit goods from a technical and economic point of view. The findings of the project presented in [42] show that the overall cost of deploying RFIDs is only 0.5% of the average price of the goods, so the impact is minimal.

Because of these described features, the market of luxury goods is likely to rely on RFID technology in the years to come, which can make the identified threats to security and privacy quite real in the long term.

To conclude, we have identified the following specific features for the use case of luxury goods:

1. The price of luxury goods is quite high for a single item, which can justify relatively sophisticated RFID deactivation techniques.
2. The deployment of RFID in luxury goods can remotely reveal the economic status of the owner, which can have both privacy and safety implications.
3. The market of luxury goods is not based on web shopping yet. It is still quite common to buy luxury goods in a shop with all the related implications for privacy.
4. The RFID can be embedded in the market of luxury goods, as opposed to surface application.
5. The luxury good cannot be damaged in any way by the RFID deactivation technique.
6. In some contexts, the owner wants to verify the authenticity of the luxury brand he bought and be able to show the proof that it is authentic (e.g., at social events); this is in opposition to other contexts where this information should not be disclosed.

3.5. Cars

There is a trend in the automotive industry to tag all the parts of a car, to ease the whole supply-chain management, but also the identification of spare parts when replacement is needed. It is also considered as important to manage the recycling at the “end of life” of the vehicle, following a Commission regulation on recycling (2000/53/EC.).

During construction of the car, many automotive factories currently use every available type of RFID system: active, passive, LF (low frequency), HF (high frequency), UHF (ultra high frequency), UWB (ultra-wide band). It is possible, but not explicitly stated by manufacturers, that the finished car at the end of the production line has some tags de-activated or removed. As

a car may host ‘hundreds’ of tags, the deactivation, or any type of anonymisation are necessary, again because of tracking and location related requirement(s).

The following industrial example may be representative of other high value goods, composed of several parts: Since 2001 RFID have been tested in various roles in the production of automotive components and complete cars, in search of greater efficiencies in production, sales and post-sale. Some of the first tentative logistic trials were made by Toyota, BMW in 2003 [43], followed by Renault [44] then Ford. BMW have since installed their trial vehicle assembly RFID systems at most of their worldwide factories.

Actual RFIDs that are deliberately introduced and maintained in the automotive sector - at and beyond the point of sale - are apparently not being considered as privacy disruptive technologies, their misuse is not widely discussed in privacy terms. Few comments, neither on privacy nor deactivation, can be found in the literature. Many of the uses of RFID in a car are considered, and can be broken down into 3 epochs: For the car’s *early life* - prior to sale to the retail customer, there are many logistical, efficiency and quality control uses from RFID.

At sale, the automotive *mid-life term* begins, where the customer is the owner. Finally the car reaches its *end of life period* - where EU/world legislation is suggesting that all components are labelled for ease of recycling.[45] We see here that RFID may be immensely useful the early and late lifecycle phases of a car; however, care must be taken of the mid-life use and potential loss of privacy from the car’s potential cloud of RFID identities on customers.

A consortium of about 20 automakers, suppliers, logistics companies, research institutes and computer software companies are developing the use of RFID in logistics and production processes in the German automotive industry within the framework of the RFID-based automotive network (RAN) project [46] Supported by the German Federal Ministry of Economics and Technology (BMWi), the companies are working together to generate a standardised implementation of RFID technology and data exchange in the German automotive industry. RAN is part of the IT beacon programme "Internet of Things" of the BMWi. This RAN project may succeed whilst the previous patchy RFID projects have not yet produced the full benefit of low-cost use of RFID identity.

Seven RAN RFID use-cases [47] have been developed and given to major partners to lead:

- Locating vehicles that have been manufactured and that are ready for pre-delivery, led by BLG Logistics, involving Daimler;
- Container & shipping Management, led by BMW;
- Just-in-Time Tier 2, Tier 1 & OEM, led by component supplier Bosch;
- Long Process Chain, led by Daimler;
- Just-in-Sequence Vehicle Seats, led by seat specialist Keiper (Johnson Controls);
- Just-in-Sequence Bumpers, led by polymer experts Rehau;
- End to End Control Manufacturing, led by Opel.

This large German industry standardisation process within RAN, in common with the previous small-scale automotive systems, uses many diverse facets of the RFID devices. The Bremen Institut für Produktion und Logistik (BIBA) is helping in the selection of tag technologies and tag locations for the RAN project. The partners have decided to use mostly the EPC Gen 2 passive ultrahigh-frequency (UHF) RFID tags, but also use other complementary RFID technologies.

An automated search of the RAN project main website for the terms ‘privacy’ and/or ‘deactivation’ produced “NO results found.” A search for ‘Merkel’ got two hits.

From the above listed RAN use-cases, it is likely that each Keiper car seat and each Rehau vehicle bumper may have an RFID identity, during at least the early and end-of-life periods. It is

not clear from the literature how the car seat or car bumper identity lifecycle is maintained during the consumer ownership period. A search of the Keiper main website for the terms 'privacy', 'RFID', and/or 'deactivation' produced "NO results found". It could be suggested to contact the Keiper data protection officer (johannes.conrad@jci.com).

A modern car such as a BMW has many consumer oriented features based around RFID. For example, RFID is used at 125 kHz for the key engine immobiliser identity; according to this model E70 document [48] up to 9 RFID antennas are located around a car for Comfort Access (keyless entry and starting) based upon encrypted data handshake signals (at 125 kHz to 868 MHz). BMW is already using RFID for their eCar initiatives/Car Sharing/Car Pooling systems. In this last case the car has RFID reader(s) which validate (a temporary) owners' rights and allows access to the car and allows the car to be driven. Car sharing clubs have a big future in large cities.

In an IEEE paper on Near Field Communication (NFC) technology (NFC is effectively 13.56 MHz RFID) [49], BMW authors address part of the privacy cloud of the RFID labelled spare-parts and components that are potentially fitted to a car by integrating an RFID reading digital wallet inside the car electronic infotainment system. "Spare Part Information increases the transparency for the customer. The packing of spare parts can be equipped with passive NFC tags storing product information. After installing the parts into the car, the information can be transferred by just holding the packing material to the dashboard Tag reader to register the spare part." For example, in case a new engine component is added - the new starter motor RFID identity tag is not integrated into the motor-hardware itself, just its transport packaging. On maintenance, the packaging RFID content is enrolled on the car dashboard computer maintained RFID wallet, then the packaging RFID is discarded and destroyed.

This wallet system would maintain the ELV EPR database, yet achieve high privacy. It is not yet clear which models of current BMW cars have this feature. BMW demonstrated this system with 4 x NXP's PN531 readers located - one in the driver exterior mirror, one in the dashboard and two located in the back seats. The standards chosen were passive Mifare ISO-14443-A RFID.

It has been reported on user generated blogs that car dealers are often attaching and reattaching uniquely coded UHF RFIDs to the car windscreen rear view mirror at point of sale and subsequent to any maintenance activities. Neither informed consent, nor any information on these RFIDs are typically supplied - it is assumed that they are a form of vehicle tracking and identification either whilst at the garage/repair premises - or some form of advanced customer recognition. People even reported the self-adhesive RFIDs being reattached upon user removal.

According to this 2009 BMW document [50] ("Damit die Prozesse auch Jahre später rückverfolgt werden können, wird der Transponder fest in die Instrumententafel eingebaut.") this implies that the instrument panel of the 3-series does feature an integrated 13.56 MHz which was built-in by the sub-component manufacturer and supplier to BMW, which is capable of being read even years later. The privacy implications of this integrated RFID transponder are not discussed in this case study.

A recent example is the RFID based Real Time Location services (RTLS) that help manufacturers to efficiently assemble the cars on the production line. Volkswagen Slovakia assembled many thousands of VWs, Audis, the Skoda Citigo and the SEAT Mii each day using a combination of technologies. Each car has an Identec i-Q350 tag applied to the inside of the vehicle's windshield, near the rear-view mirror at a 'cloning station'. This tag is an active UHF tag. The car already has a passive RFID attached during assembly; the active and passive tags are linked with the car's details in the "noFilis CrossTalk" software residing in Volkswagen Slovakias. The tag ID's are linked to the car's vehicle identification number (VIN) along with other details, such as its colour. The Identec i-Q350 communicates using UHF (868 to 915 MHz)

with a 500 metre range, does location tracking (at 2.45 GHz) with a 100 metre range and location portal crossing (with 125 kHz signals). Before a vehicle exits the VW Bratislava facility, its i-Q350 tag is removed. “If staff members forget to detach it, the tag is activated by an i-Mark position marker and transmits a signal that is interrogated by an i-Port M350 reader portal at the exit, at which time the Identec software triggers the illumination of a warning light that prompts employees to stop the car and remove the tag.” [51] The fate of the passive RFID and other tags used during assembly by VW is not defined in the literature.

BMW’s similar but older RTLS is based on magnetic Active RFID beacons which are attached to the car body shell on it entering the manufacturing plant. BMW has chosen Ubisense UWB RFID which is encoded and sends the car’s VIN number as short signals (at 6 to 8 GHz). Once the factory's quality-control department approves a vehicle after assembly and possible re-work, the tag is removed and the BMW emblem is placed on the hood. The tag can then be reused on another car. [52] It is not defined in the available scientific nor consumer literature what is the status of the other potential RFID tags which may be present in the finished BMW.

It seems that with the launch of the RAN process in Germany that automotive industrial RFID processes will soon be ubiquitous in the consumer realm. Some manufacturers have integrated some good ideas (NFC wallets, BMW) in the car; many manufacturers are, however, focusing simply on improving their own supply logistics. The environmental labelling of all components under laws similar to the End-of-Life-Vehicles (ELVs) Extended Producer Responsibility (EPR) following 2000/53/EC of 18th September 2000 unfortunately gives a negative incentive for RFID deactivation at the point of sale. RFIDs might still be slightly too expensive for all car components to be yet labelled. It is noticed that mostly freight, road haulage and transport companies are fully RFID labelling (for example: Mitsubishi heavy goods engine components [53], Michelin London Bus Tyres [54]) this labelling is not yet common at the customer level.

It seems there is little evidence yet available concerning preparedness in the automotive sector for routine deactivation at the point of sale or the use of alternative privacy enhancing techniques. A dialog with identified stakeholders in the car-industry is suggested to further enhance knowledge in this area. There have been no identified privacy enhancing solutions proposed in the automotive industry other than the proposed in-dashboard wallet by a single manufacturer, and it is still not clear how deactivation of RFID tags following the 2009 EC recommendation is or is not in conflict with the 2000/53/EC of 18th September 2000.

3.6. Association of deactivation techniques with a scenario

The assessment of the privacy dimension is assessed combining deactivation techniques with the scenarios 3.1 to 3.5 which are in the focus of this report. The following table shows the aggregated answers from the questionnaires.

Scenario[1] vs. Available Deactivation Techniques	Textile	Books	Large distribution (Supermarket)	Luxury Goods	Cars
Tags operating after POS					
Tag data modification[2]	Yes	Yes	-	Yes	-
Password-regulated access	Yes	Yes	-	Yes	-
Reduced working range	Yes	Yes	-	Yes	-
Tags not operating after POS					
Kill command	Yes	Yes	-	Yes	-
Antenna destruction	Yes	No	-	No	-
Tag destruction	Yes	No	-	No	-
Antenna removal	Yes	No	-	No	-
Tag removal	No	No	-	No	-

'Yes' means a technique is applied in the scenario and a 'No' means it is currently not applied or can not be applied. Empty fields mean that it was not possible in the course of this report to gather any information.

4. Privacy discussion of deactivation techniques related to scenarios

By February 2011, a RFID PIA Framework was developed by a consortium of major international industry bodies and endorsed by the Article 29 Data Protection Working Party and the European Commission [58]. RFID operators throughout Europe are asked to comply with the co-regulatory data protection standard procedures outlined in the PIA Framework. The bodies that signed the PIA Framework include: Association of Automatic Identification and Mobility (AIM Global), The German Federal Association for Information Technology, Telecommunications and New Media (BITKOM), The European Network and Information Security Agency (ENISA), GS1 Global, European Round Table (ERRT), European American Business Council and EuroCommerce. In addition, many organizations from Europe as well as from the US have participated in the formulation of the PIA Framework. These include: The German Federal Office for Information Security (BSI), Gerry Weber, Volkswagen, The Federal Office for Data Protection and Freedom of Information (BfDI), the European Digital Rights

[1] Scenario**:** a scenario refers to a situation/context where a technique is applied.

[2] For instance reducing the traceability erasing the unique identifier at the point of sale and leaving only generic information

Association (EDRI), Vienna University of Economics and Business (WU Vienna), Carrefour (France), Oracle (US), Deutsche Post (Brussels) and McKenna Long & Aldridge (US). Many of them were considered relevant stakeholder for this report (see annex 3).

The goal of the RFID PIA Framework is "to help RFID Application Operators uncover the privacy risks associated with an RFID Application, assess their likelihood, and document the steps taken to address those risks". As such it was consulted and used as a guideline to develop jointly with the Vienna University of Economics and Business a basic assessment and comparison of RFID deactivation techniques in respect to their privacy protection dimension.

4.1. Findings and learning from the questionnaires and interviews

The initial idea was to organise in autumn 2012 a workshop to offer to relevant stakeholders the opportunity to present available RFID deactivation techniques. It was foreseen during the workshop to discuss and assess these techniques and rank the best ones, according to the five given scenarios. It was planned to:

- Test / challenge available and realistic solutions in various scenarios with the end users
- Discuss and converge with the stakeholders on available and suitable technical solutions
- Build a realistic picture of the current implementation.

The planned objective of the workshop was to identify and assess the Best Available Techniques (BAT's) for deactivating tags at the point of sale in the retail sector. These techniques should ideally be:

- Privacy-friendly,
- Data Protection friendly,
- Security-friendly and
- Economically viable to provide EU companies with a competitive advantage on the global RFID marketplace.
-

It was planned to bring together invited stakeholders such as RFID chips and RFID readers manufacturers, RFID end users in the supply chain, merchants owning the point of sales and, to a limited extent, academia. It was the intension to facilitate an open and constructive debate between all of them.

The workshop had to be cancelled due to a very low number of participants. A questionnaire (see annex 2) was developed to gather relevant information for this deactivation study in a more cost saving manner. The questionnaire was distributed together with the workshop invitation to all identified stakeholders listed in annex 3. The response received on the questionnaire was similarly low as for the workshop. The questionnaire was only compiled by 3 supporters of the study. Though RFID technology in the retail sector had had enormous publicity some years ago, only very little representatives are implementing the recommendation and foreseeing the deactivation of the tag.

4.2. Classification of the impact to the client and the retailer

The basis of the following matrixes was developed with support from the Vienna University of Economics and Business. The objective is an evaluation of the risks (lines) associated with the deactivation techniques (columns) explained in chapter 2.

The idea behind is to assess and compare the RFID deactivation techniques in respect to their privacy protection dimension.

A 'Y' standing for yes means that the risk is seen associated at the given level with a deactivation technique. An 'N' means the opposite, which is that the risk is not seen. If there was no clear yes / no evaluation possible then a comment is put into the cell of the matrix. An empty matrix cell means that no assessment was possible with the information available. The classification in the matrixes in the following chapters is based on the answers of the questionnaire, on the literature and on the expertise of the authors. As the number of answers in the questionnaire is very low the results should not be considered statistically proved.

The metrics for the qualitative evaluation of the deactivation techniques are defined as following:

- *Transaction Cost* represents the effort to execute the deactivation technique in terms of economic impact (money) or complexity (time, organizational changes in the distributor point of sale).

- *Consumer Perception* represents the potential loss of trust due to the execution of the deactivation techniques. For example, the perception that the acquired good is damaged by the technique.

- *Attacker Resources* represents the efforts and resources (e.g., technical equipment, knowledge) that the attacker must use to implement the attack.

- *Reversibility* represents the capability of reversing the deactivation technique. In some cases, this may be impossible (e.g., the RFID has been physically destroyed or degraded). Note that the implementation effort and cost in the distributor chain to reverse the deactivation may not be the same as at the point of sale, because this action can be implemented only in specific components of the distribution chain (e.g. customer support) and the amount of reverse deactivation can be much smaller than deactivation.

4.2.1. In the textile scenario

In this scenario the RFID is attached or integrated in textiles or accessories. The deactivation technique applied in textiles needs to cope with very flexible carrier materials and the possibly simultaneous presence of having many tags very closed to each other at the POS.

	Tag Data Modification	Password Access	Reduced working range	Kill Command	Antenna or Tag destruction	Antenna or Tag removal
Transaction Cost						
low transaction cost	Y	N	Y	N	N	N
high transaction cost	N	Y	N	Y	Y	Y
Consumer Perception						
Potential loss of trust: low risk	N	N	N	N	Y	Y
Potential loss of trust: high risk	Y	Y	Y	Y	N	N
Attacker Resources						
strong attacker	Y	Y	Y	Impossible	Only for the Antenna destruction	Only for the Antenna removal
weak attacker	N	N	N	N	N	N
Reversibility						
easy	N	N	Y	N	N	N
difficult	Y if data still existing	Y	N	Y	For Antenna destruction	For Antenna removal
impossible	N	N	N	N	For Tag destruction	For Tag removal

The matrix shows that regardless the deactivation technique used the resources of an attacker will always have to be at least high. At the same moment almost all techniques are reversible. The price of the textile is typically between low and high. This combined with the expected destruction of the tag during the lifetime of the textile due to environmental influence is making the costumers easier accepting RFID tags in textile.

4.2.2. In the Book Shops Scenario

The specific aspect of this scenario is that the RFID is usually glued on the cover or inside the book. The deactivation technique applied on the book should not damage it in any form.

	Tag Data Modification	Password Access	Reduced working range	Kill Command	Antenna or Tag destruction	Antenna or Tag removal
Transaction Cost						
low transaction cost	Y	Y	Y	Y	Y	Y
high transaction cost	N	N	N	N	N	N
Consumer Perception						
Potential loss of trust: low risk	Y	Y	Y	Y	Y	Y
Potential loss of trust: high risk	N	N	N	N	N	N
Attacker Resources						
strong attacker	Y	Y	Y	-	-	-
weak attacker	N	N	N	-	-	-
Reversibility						
easy	Y	Y	Y	N	N	N
difficult	N	N	N	N	N	N
impossible	N	N	N	Y	Y	Y

The matrix shows that regardless the deactivation technique used the transaction costs will always have be low and as such it will be like to be beneficial for manufacturers to be used. Though the consumer perception was evaluated always as low risk an in-depth analysis would be required to possible profiling especially in respect to religious and medical literature.

4.2.3. Large distribution

The specific aspect of this scenario is that the RFID is usually attached to very different products or covers. The deactivation technique applied in large distributions needs to cope with very different carrier materials and also with the simultaneous presence of a high number of tagged goods very closed to each other.

	Tag Data Modification	Password Access	Reduced working range	Kill Command	Antenna or Tag destruction	Antenna or Tag removal
Transaction Cost						
low transaction cost	Y	Y	Y	Y	N	N
high transaction cost	N	N	N	N	Y	Y
Consumer Perception						
Potential loss of trust: low risk	Y	Y	Y	Y	Y	Y
Potential loss of trust: high risk	N	N	N	N	N	N
Attacker Resources						
strong attacker	Y	Y	Y	-	-	-
weak attacker	N	N	N	-	-	-
Reversibility						
easy	Y	Y	Y	N	N	N
difficult	N	N	N	N	N	N
impossible	N	N	N	Y	Y	Y

The expectations from the consumer in respect to time savings are in the scenario the biggest in comparison to the other 4 scenarios assessed. The matrix does not show a clear situation, which indicates that the risk differs very much, and it is associated with the concrete implementation. It will never make sense to apply some techniques in that scenario as the handling will not be adequate for the process targets. It will simply not be accepted to remove mechanically antenna or tag from a big number (<= 50) by hand.

4.2.4. In the Luxury goods scenario

The specific aspect of this scenario is that the RFID is usually embedded in the structure of the luxury goods and any deactivation method based (reduced working range, antenna or tag destruction, antenna or tag removal) on the physical modification of the RFID tag has an high risk of damaging the luxury good. In addition, this scenario also presents a high risk of loss of trust by the customer due to the perceived alteration of the goods, even if this is not practically true (only the RFID is altered).

	Tag Data Modification	Password Access	Reduced working range	Kill Command	Antenna or Tag destruction	Antenna or Tag removal
Transaction Cost						
low transaction cost	Y	Y	N	Y	N	N
high transaction cost	N	N	Y	N	Y	Y
Consumer Perception						
Potential loss of trust: low risk	N	N	N	Y	N	N
Potential loss of trust: high risk	Y	Y	Y	N	Y	Y
Attacker Resources						
strong attacker	Y	Y	N	Y	Y	Y
weak attacker	N	N	Y	N	N	N
Reversibility						
easy	Y	Y	N	Y	N	N
difficult	N	N	Y	N	N	N
impossible	N	N	N	N	Y	Y

This is besides the car scenario the one for which the interest of the consumer to agree on a non-deactivation of the tag might be the biggest. The consumer will be in the possession to prove the origin of the high valuable good and might want to use this as well to prove his legal ownership. Contrary to this there will clearly be situations where the consumer insists on a 100% protection of his privacy, for example not to reveal the presence of high values belonging to him in a given area. The interest of the attacker in this scenario - given economically beneficial situations - is considered the highest of all 5 compared scenarios.

4.2.5. In the automotive industry (cars scenario)

The specific aspect of the car scenario is that a high number of RFIDs are embedded in the structure of the car and its components. The deactivation technique needs to be seen as a unit of the function of the car with a high interest to use it for after sale services.

	Tag Data Modification	Password Access	Reduced working range	Kill Command	Antenna or Tag destruction	Antenna or Tag removal
Transaction Cost						
low transaction cost	N	N	N	N	N	N
high transaction cost	Y	Y	Y	Y	Y	Y
Consumer Perception						
Potential loss of trust: low risk	N	N	N	N	N	N
Potential loss of trust: high risk	Y	Y	Y	Y	Y	Y
Attacker Resources						
strong attacker	Y	Y	Y	N	N	Y
weak attacker	N	N	Y	N	N	N
Reversibility						
easy	Y	Y	Y	N	N	N
difficult	Y	Y	Y	Y	Y	Y
impossible	N	N	N	Y	Y	Y

This is besides the luxury goods scenario the one for which the interest of the consumer to agree on a non-deactivation of the tag might be the biggest. The car industry is using the tags on a wide basis for maintenance purposes. The consumer perception is for all techniques classified as of high risk. This comes mainly from the price of a car and its technical complexity.

4.3. Mitigating the risks: proposals of countermeasures to scenarios

Four basic risks were considered in the classification as described in chapter 4.2. The risks are intrinsically connected to the type of RFID handling at the POS for deactivation and after the POS. All techniques destroying the tag can not be used for after sales services but are guaranteeing a 'no risk' for the customer. Techniques leaving the tag operational after the POS instead can be used under certain conditions for after sales services.

The transaction cost has mainly an economic impact but in some conditions may affect the feasibility by creating too high constraints (queue, delays, and resources) inducing design effort to select the appropriate technique where technically/economically possible. Information campaigns and education of the public needs to be used to develop consumer perception (see chapter 4.4).

Attacker resources needed to attack the technology are typically decreasing with the technological development and the wide information exchange, for example, on the internet about the attack. Priority should be given to techniques which are intrinsically irreversible. The limitation here is to integrate them into after sales activities. The maturity of the technique plays also an important role. This counts especially for the level of the standardisation of the technique. From the technical perspective, the revision of ISO 18006 can be seen as very relevant as it may offer new perspectives for the adoption of new crypto mechanisms.

4.4. Public Awareness and Education

EU and stakeholders initiatives address different aspects of improving the public awareness regarding RFID tags in the retail sector, as a means to allow this technology to fulfil its economic promise. At the same time, it is very important to work on the mitigation of the risks, in order to avoid having it being used to the detriment of the public interest, thus enhancing its acceptability.

DiscoverRFID for example is a website [66] created in 2008 by GS1 EPCglobal to raise awareness of the general public on the benefits of RFID. The RFID Educational Foundation [67] aims to educate and inform the general public, consumers, and others about RFID technology and promotes public awareness about RFID technology capabilities and limitations.
At the end it will be the costumer who needs to accept the presence of active or deactivated RFIDs on retail products and as such public awareness and education is key for the success of the use of RFID technology.

5. Conclusions

The present study has been prepared for DG CNECT asking JRC to report by the end of 2012 on the RFID deactivation techniques at the point of sale.

The different available techniques have been identified and described, mainly into 2 classes: Tags operating after the POS and Tags *not* operating after the POS.

A large operation of information mining has been deployed (direct contact and contact with associations, visits to industry and operators, diffusion of a questionnaire, organization of a workshop), in order to collect the necessary input from the stakeholders regarding the use and the implementation of these techniques.

The collection of information resulted very difficult. The authors of the report have regardless of their effort not been able to involve a statistically solid number of stakeholders. The response dynamic received for the workshop and for the questionnaire was very low. Though RFID technology in the retail sector had had enormous publicity some years ago, only very little operators are nowadays implementing the recommendation and foreseeing the deactivation of the tags.

Nevertheless, and like illustrated in the 5 scenarios developed in this study, the adoption of RFID tags in the supply chain offers clear opportunities: tracking the whole course of the product existence, from manufacturing to storage, through sale, after sale and products usage, with the identified need to be deactivated at the POS.

From what we perceived, the implementation of RFID technology is still limited. In particular this may be explained by the following arguments:

- Public acceptance of the technology
- Price of RFID tags and its associated possible cost savings
- Harsh environment for example in the textile production (high temperatures, chemicals, physical processing) or for the car manufacturing
- It cannot be excluded that the recommendation created some hesitation in the industry and by the retailers regarding the use of RFID tags

At the other hand, it is expected that the deactivation of the RFID at the POS as recommended by the European Commission will be key in improving the acceptance of the technology among the consumers (more trust and less fear regarding privacy issues).

Regarding the implementation, the market is characterized by a number of fragmented proprietary tailor-made RFID systems, almost prototypes and in pilot phases, but rarely deployed on a wide basis. To this respect, the current standardization effort is most probably the better answer.

To deploy RFID tagging, including workable deactivation processes in various scenarios of the retail market, RFID manufacturers and system integrators have to work on reducing the process time and improving the security. During the system planning and design they have to work closely with the retailers and store managers in order to find the best solution using the best available deactivation technique to satisfy the need of each actor/stakeholder in the supply chain, from assembly plants to final customer.

The authors of the study note that the implementation of the RFID recommendation is following strong economic and strategic constraints. Retailers/Operators are currently adjusting their efforts to maintain a positive image while guaranteeing their profits. The benefit for the consumer is at that stage questionable.

Annex 1: References

[1] Gemalto, “The difference between contactless smart cards & RFID tags”, online reference, 2012. http://www.gemalto.com/brochures/education/download/contactless_RFID.pdf

[2] Smart Card Alliance, “Contactless Smart Cards vs. EPC Gen 2 RFID Tags: Frequently Asked Questions”, online reference, 2012. http://www.smartcardalliance.org/resources/pdf/EPC_Gen_2_FAQ_FINAL.pdf

[3] GS1, “GS1 EPC Tag Data Standard 1.6”, 2011. Available online at http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf.

[4] Mikko Lehtonen, Antti Ruhanen, Florian Michahelles, and Elgar Fleisch. “Serialized TID numbers - A headache or a blessing for RFID crackers?”, in IEEE International Conference on RFID 2009, pp.233-240, IEEE, 2009.

[5] European Commission, “On the implementation of privacy and data protection principles in applications supported by radio-frequency identification”, Commission Recommendation, 12/05/2009.

[6] Ari Juels, “RFID Security and Privacy: A Research Survey”, RSA Laboratories, 2005. Available online at http://www.rsa.com/rsalabs/staff/bios/ajuels/publications/pdfs/rfid_survey_28_09_05.pdf

[7] ISO/IEC 15693, “Identification cards - Contactless integrated circuit cards - Vicinity cards”, ISO/IEC Standard.

[8] ISO/IEC 18000-3, “Information technology - Radio frequency identification for item management - Part 3: Parameters for air interface communications at 13,56MHz”, ISO/IEC Standard.

[9] ISO/IEC 18000-61, “Information technology - Radio frequency identification for item management - Part 61: Parameters for air interface communications at 860MHz to 960MHz Type A”, ISO/IEC Standard.

[10] ISO/IEC 18000-62, “Information technology - Radio frequency identification for item management - Part 61: Parameters for air interface communications at 860MHz to 960MHz Type B”, ISO/IEC Standard.

[11] ISO/IEC 18000-63, “Information technology - Radio frequency identification for item management - Part 61: Parameters for air interface communications at 860MHz to 960MHz Type C”, ISO/IEC Standard.

[12] ISO/IEC 18000-64, “Information technology - Radio frequency identification for item management - Part 61: Parameters for air interface communications at 860MHz to 960MHz Type D”, ISO/IEC Standard.

[13] GS1, “EPCglobal Object Name Service (ONS) 1.0.1”, 2008. Available online at http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_1_0_1-standard-20080529.pdf.

[14] Gerhard Hancke, "Practical eavesdropping and skimming attacks on high-frequency RFID tokens", in Journal of Computer Security 19, no. 2, pp.259-288, 2011.

[15] Harko Robroch, “ePassport Privacy Attack”, Riscure presentation at Cards Asia Singapore, April 2006. Available online at http://www.riscure.com/archive/200604_CardsAsiaSing_ePassport_Privacy.pdf.

[16] Davide Zanetti and Danev Boris, "Physical-layer identification of UHF RFID tags", in Proceedings of the sixteenth annual international conference on Mobile computing and networking, pp.353-364, ACM, 2010.

[17] Danev Boris, Thomas S. Heydt-Benjamin and Srdjan Capkun. "Physical-layer identification of RFID devices", in Proceedings of the USENIX Security Symposium, pp.199-214, 2009.

[18] Gildas Avoine and Philippe Oechslin, "RFID traceability: A multilayer problem", Financial Cryptography and Data Security, pp.577-577, 2005.

[19] Ari Juels and Stephen Weis, "Defining strong privacy for RFID", in Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, pp.342-347, IEEE, 2007.

[20] Sanjay Sarma, Stephen Weis and Daniel Engels, "RFID systems and security and privacy implications", Cryptographic Hardware and Embedded Systems CHES 2002, pp.1-19, 2003.

[21] Sozo Inoue and Hiroto Yasuura, "RFID privacy using user-controllable uniqueness", 2003.

[22] Yossef Oren and Adi Shamir, "Remote password extraction from RFID tags", IEEE Transactions on Computers, 56(9), pp.1292-1296, 2007.

[23] Paul A. Moskowitz, Andris Lauris and Stephen Morris, "A privacy-enhancing radio frequency identification tag: Implementation of the clipped tag", in Fifth Annual IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 348-351, IEEE, 2007.

[24] United States Patent 7,253,734, “System and method for altering or disabling RFID tags”, USPTO, 2007.

[25] Günter Karjoth and Paul A. Moskowitz, "Disabling RFID tags with visible confirmation: clipped tags are silenced", in Proceedings of the 2005 ACM workshop on Privacy in the electronic society, pp. 27-30, ACM, 2005.

[26] “SmartCode Corp. Solves Privacy Issue Relating To Potential Unauthorized Reading Of RFID Enabled Passports And ID Cards”, online reference 2012. http://www.rfidsolutionsonline.com/doc.mvc/SmartCode-Corp-Solves-Privacy-Issue-Relating-0001.

[27] Alanson P. Sample, Daniel J. Yeager and Joshua R. Smith, "A capacitive touch interface for passive RFID tags", in 2009 IEEE International Conference on RFID, pp. 103-109, IEEE, 2009.

[28] Alexei Czeskis, Karl Koscher, Joshua R. Smith and Tadayoshi Kohno, "RFIDs and secret handshakes: Defending against ghost-and-leech attacks and unauthorized reads with context-aware communications", in Proceedings of the 15th ACM conference on computer and communications security, pp. 479-490, ACM, 2008.

[29] Ari Juels, Ronald L. Rivest and Michael Szydlo, "The blocker tag: Selective blocking of RFID tags for consumer privacy", in Proceedings of the 10th ACM conference on computer and communications security, pp. 103-111, ACM, 2003.

[30] Impinj, “QT Technology”, online reference, 2012. http://www.impinj.com/QT_Technology.aspx.

[31] Ari Juels, "Minimalist cryptography for low-cost RFID tags", Security in Communication Networks, 149-164, 2005.

[32] Miyako Ohkubo, Koutarou Suzuki and Shingo Kinoshita, "Cryptographic approach to “privacy-friendly” tags", in RFID Privacy Workshop, vol. 82, MIT, Cambridge, MA, 2003.

[33] Stephen Weis, Sanjay Sarma, Ronald Rivest and Daniel Engels, "Security and privacy aspects of low-cost radio frequency identification systems", Security in pervasive computing, pp.50-59, 2004.

[34] Ari Juels and Ravikanth Pappu, "Squealing Euros: Privacy protection in RFID-enabled banknotes", in Computer Aided Verification, pp. 103-121, Springer Berlin/Heidelberg, 2003.

[35] Dirk Henrici and Paul Muller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers", in Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops, pp.149-153, IEEE, 2004.

[36] Tassos Dimitriou, "A lightweight RFID protocol to protect against traceability and cloning attacks", in First International Conference on Security and Privacy for Emerging Areas in Communications Networks - SecureComm 2005, pp.59-66, IEEE, 2005.

[37] Philippe Golle, Markus Jakobsson, Ari Juels and Paul Syverson, "Universal re-encryption for mixnets", Topics in Cryptology–CT-RSA 2004.

[38] Giuseppe Ateniese, Jan Camenisch and Breno de Medeiros, "Untraceable RFID tags via insubvertible encryption", in Proceedings of the 12th ACM conference on Computer and communications security, pp.92-101, ACM, 2005.

[39] C (2012) 1342 final, COMMISSION RECOMMENDATION of 9.3.2012 on preparations for the roll-out of smart metering systems

[40] J. Park, J. Jung, S. Ahn, H. Roh, H. Oh, Y.R. Seong, Y Lee and K. Choi, “Extending the interrogation range of a passive UHF RFID system with an external continuous wave transmitter,” IEEE Instrumentation and Measurement Transaction, vol. 59, August 2010, pp.2191–2197.

[41] Luxury Apparel Maker to Test TexTrace's Fabric RFID Label. http://www.rfidjournal.com/article/view/9415/2. Last Accessed 5 November 2012.

[42] FP6 BRIDGE Building Radio frequency IDentification for the Global Environment - Anti-counterfeiting Business Case Report. http://www.bridge-project.eu/data/File/BRIDGE_WP05_Anti_counterfeiting_business_case_report.pdf. Last Accessed 5 November 2012.

[43] Jonathan Collins, September 20, 2005, http://www.rfidjournal.com/article/print/1877

[44] Renault Benefits from Using RFID for Quality Control Luc Filizzola, RFID Production Manager, Renault Dominique Hardier, Manager of Manufacturing Information Systems, Renault http://www.rfidjournalevents.com/live/casestudy.php

[45] Automotive green supply chain management based on the RFID technology Tongzhu Zhang, IEEE International Conference on Advanced Management Science (ICAMS), 2010 End-of-Life-Vehicles (ELVs) Extended Producer Responsibility (EPR) following 2000/53/EC of 18th September 2000.

[46] http://www.autoran.de/en/home.html Die Prozesse der Automobilindustrie transparent und optimal steuern, RAN Project Manager: michael.patocka@daimler.com

[47] Rhea Wessel, July 11, 2011, http://www.mojix.com/news/2011/rfidjournal-article8587.PDF

[48] BMW technical note for the E70 RFID systems (E70 is the development name for the current X5 Sports Activity Vehicle) http://www.bmwmotorsports.org/pdf/e70/05a3_E70%20Comfort%20Access.pdf

[49] "Near Field Communication (NFC) in an Automotive Environment" , IEEE Second International Workshop on Near Field Communication, 2010 BMW Group Research and Technology Munich, Germany. Corresponding author: rainer.steffen@bmw.de

[50] http://www.rfidatlas.de/images/stories/bmw_februar2009.pdf Case study - BMW Group

[51] According to Claire Swedberg June 13, 2012, http://www.rfidjournal.com/article/print/9614

[52] Claire Swedberg August 4, 2009, http://www.rfidjournal.com/article/print/5104

[53] "Parts Maker Uses RFID to Increase Efficiencies" Chris Page, Senior Business Manager, Midtronics Adam M. Warmack, Account Manager, Mitsubishi Electric Automotive America

[54] Michelin embeds EPC Gen 2 passive ultrahigh-frequency (UHF) radio frequency identification tags into tire sidewalls during the manufacturing process, enabling the London city's bus-fleet operators, or the tire manufacturer's staff, to use RFID to automatically identify each tire when its pressure is being measured.

[55] M Senthilkumar, et. al., Concept & applications of RFID in textile & apparel industry, The Indian Textile Journal, March 2010, http://www.indiantextilejournal.com/articles/FAdetails.asp?id=2738

[56] Study on labeling of textile products, European Parliament, DIRECTORATE GENERAL FOR INTERNAL POLICIES, POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICIES, INTERNAL MARKET AND CONSUMER PROTECTION, IP/A/IMCO/ST/2009, 11 JANUARY 2010, PE 429.992

[57] http://www.rfid-library.com/en/default_e.html

[58] European Commission (EC): Privacy and Data Protection Impact Assessment Framework for RFID Applications. 12 January 2011.

[59] Federal Office for Information Security (BSI): IT-Grundschutz Catalogues: Layer 1 B1.5 Data protection. 2005.

[60] Bartels, C., Kelter, H.: Technical Guidelines for Implementation and Utilisation of RFID-based Systems. ISSE/SECURE2007, Securing Electronic Business Processes, Vieweg-Verlag 2007, ISBN 978-3-8348-0346-7.

[61] Federal Office for Information Security (BSI): TG 03126 - Technical Guidelines for the Secure Use of RFID. TG 03126-4 Application area "trade logistics". 2008.

[62] Federal Office for Information Security (BSI): TG 03126 - Technical Guidelines for the Secure Use of RFID. TG 03126-1 Application area "eTicketing in public transport". 2009.

[63] Federal Office for Information Security (BSI): Technical Guideline TR-03126-5. Technical Guidelines for the Secure Use of RFID (TG RFID). Subdocument 5: Application area “Electronic Employee ID Card”. Version 1.0, 2010.

[64] European Parliament and the Council (EC): Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. 24 October 1995.

[65] Ward Jeurissen, RFID Adoption in Bookstores - A study on factors that explain adoption intention, University of Twente, School of Management and Governance, Business Administration – Innovation Management, 2008

[66] http://discoverrfid.org/

[67] http://www.therfidfoundation.org

Annex 2: Questionnaire

"RFID deactivation at the point of sale in the retail sector"

Questionnaire - Techniques vs. Scenarios

October 2012 – Ver. 4.1

Background

In 2009 the EC published the Commission Recommendation on data protection, privacy and security aspects of RFID (COMMISSION RECOMMENDATION of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification). Over the last two years, the EC has successfully contributed to the implementation of several clauses in the Recommendation, by initiating and participating in a co-regulation process (RFID Privacy Impact Assessment) and by issuing a Mandate (M/436) requesting European Standardisation Organisations to address some relevant standards gaps (emblem and signage, device privacy, Privacy Impact Assessment (PIA), security, extended device capability). The same recommendation foresees that the EC reports after 3 years on specific provisions of the implementation: status on PIA's, standardization, logo, and deactivation at the point of sale (POS).

The JRC is in charge of editing a report for DG CNECT, for the end of this year 2012, on the deactivation at the POS in the retail sector: implementation, and discussion on the Best Available Techniques (BATs).

Questionnaire

The attached questionnaire intends to collect technical, procedural and economical information, basically facts from relevant stakeholders such as RFID chips and readers manufacturers, RFID end users in the supply chain, merchants owning a POS and, to a limited extent, academia. The questions are covering a wide range of expertise and as such it is not required that each stakeholder answers all questions (please select the questions relevant to your expertise).

Motivation and Objectives

The questionnaire has been prepared having in mind specific objectives. From the answers, and a subsequent processing, including anonymization of the data collected, it is intended to:

- Build a realistic picture of the current implementation
- On a given set of representative scenarios, test/challenge the implementation of available and realistic solutions
- Identify and assess the Best Available Techniques for deactivating tags at the POS, taking into account the Privacy and Data Protection dimension, the security of the individuals, and the economic viability of the solutions (competitive advantage for EU companies on the global RFID marketplace)

Set of representative scenarios

Textile: large diffusion of consumer textile goods, with issues regarding identification, tracking and location. Clients may wish to return the goods.

Books: Book shops environment. Natural extension for books loan in libraries. The book content may have a specific significance regarding Religion, Personal preferences, Medical interest.

Large distribution: low nominal cost goods. The solution for deactivation needs to be low cost as well, and the speed at the point of sale is an economic parameter.

Luxury goods: deactivation solution may be expensive, and speed at the point of sale is less an issue, but the deactivation is challenging, as Security, Fraud, Theft, Tracking and Product authentication are at stake.

Automotive industry (cars): supply-chain management, identification of spare parts when replacement is needed and managing the recycling at the "end of life" push for massive tagging. As a car may therefore host 'hundreds' of tags, deactivation or any type of anonymisation provisions are necessary (tracking and location related issues).

Techniques versus Scenarios matrix:

The following table associates deactivation techniques with the scenario in focus. The aim is to acquire which techniques are in use for a given process. We expect simple yes/no answer in the fields where you feel competent. Additional comments can be given below in case a yes/no is not enough.

Scenario[3] vs. Available Deactivation Techniques	Textile	Books	Large distribution (Supermarket)	Luxury Goods	Cars
Tags operating after POS					
Tag data modification[4]					
Password-regulated access					
Reduced working range					
Tags not operating after POS					
Kill command					
Antenna destruction					
Tag destruction					
Antenna removal					
Tag removal					

[3] Scenario**:** a scenario refers to a situation/context where a technique is applied.

[4] For instance reducing the traceability erasing the unique identifier at the point of sale and leaving only generic information

Comments:

Questions relating to RFID tags characteristics and specifications

Q1: On which typical support material the RFID is applied (plastic, metal, paper)?

Q2: Number of foreseen tag (millions, billions of tags before an identifier will repeat)?

Q3: What is the nominal minimal & maximal RFID read distance?

Q4: What is the maximum number of tags which can be quasi simultaneously deactivated?

Q5: Which supply chain information is stored in the tag?

Q6: Is a deactivation tool needed (reader / writer, scissors or punch)?

Q7: Does the deactivation require specific capabilities from the deactivation operator for a correct deactivation (e.g. cut right on the chip and not only on the antenna)?

Q8: Is the successful deactivation verifiable for the customer of the tag with an RFID?

Q9: Are you taking into consideration any possible privacy issues at any level during tag-reader interactions? (e.g., are static tag-identifiers used during singulation protocols?)

Q10: Is the tag memory write-locked? (e.g. avoiding the possibility for an attacker to store his/her unique ID)

Q11: Is the communication from the reader to the tag encrypted? (i.e. eavesdropping possibility)

Q12: Do you see any additional deactivation technique to mention?

Q13: Is the deactivation reversible?

Q14: Is the deactivated tag identifiable?

Q15: Is the deactivated tag traceable?

Q16: Typical time for 1 tag deactivation?

Q17: Typical time for 10 tags deactivation?

Q18: Typical time for 500 tags deactivation?

Q19: How long is the time to validate successful deactivation?

Q20: How long is the time to validate a non successful deactivation?

Q21: What is the applicable temperature range for the deactivation system?

Q22: What is the applicable humidity range for the deactivation system?

Q23: What is the nominal RF field strength at the approximate position of the tag deactivator at the moment of deactivation?

Q24: What is the nominal RF field strength at the approximate position of the buyer of the tagged good at the moment of deactivation?

Questions relating to operational and organisational provisions at the point of sale (POS):

Q25: In few words, how are you handling the RFID deactivation at the point of sale (POS)? Supporting information like project descriptions, flyers or other documentation is welcome.

Q26: What is the process to obtain consent from the buyer not to deactivate the tag?

Q27: How are returned goods handled after deactivation of the RFID?

Q28: Are specific chip capabilities required for the merchant (e.g. crypto)? Example?

Q29: Are there additional constraints featuring the implementation of your solution? (e.g. password management)

Q30: Are you applying any Privacy Impact Assessment (PIA) to identify and mitigate privacy issues?

Q31: Is the deactivation delaying your process at the point of sale (POS) and if so by how much?

Q32: Is the tag active/available for after sales services?

Q33: What would be the estimated price for your deactivation system at one point of sale?

Q34: What would be the estimated price / tag in your solution?

Q35: What would be the estimated price / reader in your solution?

Q36: What would be the estimated price / deactivation tool if applicable?

Q37: Is the RFID tag re-usable for other purposes after e.g. removal?

Q38: JRC is applying the process to define Best Available Techniques for tag deactivation in the retail sector at the point of sale, according to the Commission Implementing Decision 2012/119/EU, taking inspiration in the Directive 2010/75/EU of the European Parliament and of the Council on industrial emissions. Do you want to be involved in the "BAT's for RFID tags deactivation" stakeholder group?

Additional information on the Recommendation Objectives

The RFID Recommendation gives particular attention to the concern about individual tracking and access to personal data in the retail sector (points 11-14), where it is feared that tagged items bought by individuals could be misused by retailers or third parties for tracking or profiling purposes. It establishes the principle that tags must be deactivated at the point of sale by default unless the customers give their informed consent to keep tags operational. However, it allows an exception to this deactivation principle if the PIA concludes that keeping tags operational after the point of sale does not represent a likely threat to privacy or the protection of personal data. The Article 29 Data Protection Working Party observed in its Opinion of 11 February 2011 that a risk management approach, as suggested by the PIA, is an essential tool for the RFID Operator to assess the risks of taking the responsibility to keep tags activated after the point of sale.

Please return this questionnaire to: jan.loeschner@jrc.ec.europa.eu

Annex 3: List of relevant stakeholders

RFID chip manufacturers:

ESIA European Semiconductor Industry Association
Infineon
NXP
STM

RFID reader manufacturers:

STid
EMBISPHERE

Merchants owning the point of sales, RFID end users in the supply chain:

AEG Identificationsystem GmbH
Decathlon
ERRT European Retail Round Table
EuroCommerce
FEIG Electronic GmbH
Gerry Webber
IDS Microchip AG
JCPenney
Marks & Spencer
Macy's
METRO
Nordic ID GmbH
Pasquini and Kromer GmbH
Plasticard-ZFT GmbH
Psion GmbH
RAKO Security-Label GmbH
SAG Security Assembly Group Co. LTD
Schreiner Group GmbH & Co KG
TexTrace
Walmart
WAROK GmbH

System Integrator:

AIM Association for Automatic Identification and Mobility
EPoSS European Tech Platform on Smart Systems Integration
Gemalto
MESOTECHNIC
Orange Labs
Philips
Tyco (NL)

RFID and standardisation related associations and exerts groups:

ANEC The European Consumer Voice in Standardisation

(BITKOM)	The German Federal Association for Information Technology, Telecommunications and New Media
BEUC	European Consumers Organisation
BSI	Federal Office for Information Security
CEN	European committee for standardisation
CNRFID	Centre National RFID
ETSI	European Telecom Standardisation Institute
ETUC	European trade union confederation
GS1	(INDICOD, Italy)
RFID I Danmark	
RFID NL	Platform Nederland

Supervisory authorities:

Article 29 group

Academia:

AIT	Athens Information Technology
AIT	Austrian Institute of Technology
Cambridge University	
EPFL	École polytechnique fédérale de Lausanne
IBM	Research Division, Zurich Research Laboratory
IERC	IoT European Research Cluster
IML	Fraunhofer-Institut für Materialfluss und Logistik
SICS	Swedish Institute of Computer Science
TNO	
Uni-Kl	University of Kaiserslautern, Germany
USI	Università della Svizzera italiana
WU	Vienna University of Economics and Business

As the Commission's in-house science service, the Joint Research Centre's mission is to provide EU policies with independent, evidence-based scientific and technical support throughout the whole policy cycle.

Working in close cooperation with policy Directorates-General, the JRC addresses key societal challenges while stimulating innovation through developing new standards, methods and tools, and sharing and transferring its know-how to the Member States and international community.

Key policy areas include: environment and climate change; energy and transport; agriculture and food security; health and consumer protection; information society and digital agenda; safety and security including nuclear; all supported through a cross-cutting and multi-disciplinary approach.