



RFID Privacy Issues

Contribution to the RFID Expert Group Meeting on 10 July 2007

by Andreas Krisch

Version: 1.1

Contents

<u>1 Preface.....</u>	<u>3</u>
<u>2 RFID Data Protection and Privacy Issues.....</u>	<u>3</u>
<u>2.1 Identification vs. Information.....</u>	<u>3</u>
<u>2.2 Enhancing Data Protection.....</u>	<u>3</u>
<u>2.3 Empowerment and Awareness Raising.....</u>	<u>4</u>
<u>3 Classification of RFID Applications.....</u>	<u>4</u>
<u>3.1 Distinction between personal and non-personal data.....</u>	<u>5</u>
<u>3.2 Distinction between open, closed and no circulation systems.....</u>	<u>5</u>
<u>3.3 Classification based on data-protection and user control.....</u>	<u>5</u>
<u>3.3.1 User control.....</u>	<u>7</u>
<u>3.3.2 Data-protection.....</u>	<u>7</u>
<u>3.3.3 Barriers.....</u>	<u>7</u>

1 Preface

European Digital Rights (EDRi), an association of 25 privacy and civil rights organisations from 16 countries in Europe, welcomes the efforts of the European Commission towards a EU policy framework for RFID. EDRi fully agrees that it is “*essential that the implementation of RFID takes place under a legal framework that affords citizens effective safeguards for fundamental values, health, data protection and privacy.*”¹ Therefore EDRi gladly contributes to the RFID Expert Group established by the European Commission.

With this paper we want to share our thoughts on RFID Privacy Issues with the members of the RFID Expert Group and propose a classification scheme for RFID applications based on data protection and user² control.

2 RFID Data Protection and Privacy Issues

2.1 Identification vs. Information

An attribute that all Radio Frequency Identification systems have in common is – as already given in the name – that they identify something or someone. This, apparently trivial, observation is important for understanding the privacy implications of a widespread use of RFID. Establishing a global **identification system** for objects will lead to a global system identifying persons that are related to objects.

In the centre of every objects lifecycle are natural persons who fulfil a certain role with regard to this object. Be it in manufacturing, transport, trade, use or disposal. In every phase of the objects lifecycle identifying an object can lead to an identification of the person(s) related to this object and collecting data on the object can mean to collect data on the related person(s).

In RFID applications identification is often only a mean to achieve the main purpose of the application, to collect and provide **information on objects**.

To achieve a privacy friendly implementation of RFID applications, it is therefore important to design RFID applications that provide the requested information on objects while limiting the identification to an absolute minimum. To this end it always has to be considered if the identification of an object is really necessary to collect or receive the information needed.

It will be important to define the person using an application as the initiator of the interaction with the system, to achieve RFID based information systems that respect their users privacy while delivering the benefits of the availability of enhanced information on objects.

2.2 Enhancing Data Protection

“Privacy and security should be built into the RFID information systems before their widespread deployment (“security and privacy-by-design”), rather than having to deal with it afterwards.”³

With a widespread use of RFID applications the collection of data will dramatically increase, while it will become more and more complicated for the affected persons to understand and overlook all these applications and the data they collect.

Therefore it is of special importance to strengthen the data protection authorities and to enable them to protect the legitimate rights of the data subjects effectively.

To this end it is not only necessary to provide a solid financial and legal basis on which data protection

1 Commission Communication “Radio Frequency Identification (RFID) in Europe: steps towards a policy framework”, COM(2007)96 final

2 The term “user” refers here to the natural person affected by the application.

3 *ibid.*

authorities are able to establish a well functioning system of active control, but also to design information systems that facilitate the inspection and control of their compliance with data protection requirements.

Purpose oriented applications with privacy friendly defaults that keep the collected data at an absolute minimum have to be the ambition of RFID information system design. Standardised interfaces for data protection authorities need to be developed to help automating the control of compliance with data protection legislation and data protection guidelines.

The establishment of standardised data protection audits, that developers and operators of RFID applications can choose to attend on a voluntary basis, will help to increase the trust in these systems. To strengthen the position of the natural persons affected by RFID applications, the unlawful collection, circulation and use of data should be considerably sanctioned.

To encourage an enhancement of RFID technology open standards are required to enable the development of a diverse set of applications by the numerous small and medium sized IT companies as well as the developers of free and open source software across Europe.

2.3 Empowerment and Awareness Raising

“RFID will only be able to deliver its numerous economic and societal benefits if effective guarantees are in place on data protection, privacy and the associated ethical dimensions that lie at the heart of the debate on the public acceptance of RFID.”⁴

Defining the person using the application as the initiator of the interaction with RFID systems requires that the users are convinced that these applications will not infringe their privacy and that accurate measures of data protection are in place.

To achieve the users trust in RFID applications, two provisions are required: effective tools that support the users protecting their personal data and privacy, and information on the systematic context of these systems.

To support the user in effectively exercising her or his data protection rights, RFID applications should provide standardised interfaces and tools, that help to control the information stored on the user. Furthermore it is important to develop adequate mechanisms for identity management that support the user in giving consent to process data on her/him and with administering this declarations of consent. Supporting legal measures may be required in this field.

The creation of privacy enabling procedures for RFID applications needs to be based on a user-friendly system design. Complex or user-unfriendly procedures will leave the users overstrained and cause the system to fail. While providing the user with an understandable user-friendly interface it is important, that the decisions related to privacy and data protection are consciously taken by the user and not delegated to machines or software that take decisions based on some sets of preferences or other parameters.

As the Online Consultation on Future RFID Technology Policy⁵ indicates, a majority (60 %) of the respondents feel that there is insufficient information available to make an informed analysis of RFID technologies.

Therefore a balanced, comprehensible and objective information on the systematic context of and the data collected by RFID applications is required as a basis for self-determined decisions.

3 Classification of RFID Applications

With regard to the classification of RFID applications EDRi would like to contribute the following considerations:

4 *ibid.*

5 RESULTS OF THE PUBLIC ONLINE CONSULTATION ON FUTURE RADIO FREQUENCY IDENTIFICATION TECHNOLOGY POLICY "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats", SEC (2007) 312

3.1 Distinction between personal and non-personal data

The definition of personal data in the Data Protection Directive⁶ includes “*any information relating to an identified or identifiable natural person*”. This includes not only information on persons stored on RFID tags or in information systems, but also information stored on objects, if this information can be linked to a natural person at any time.

As a consequence, in RFID applications this means that the same piece of information can be either personal or non-personal, depending on the circumstances. If a product is identified by a unique identification number (ID), which is used to track the movement of the product along the supply chain, the collected data is considered non-personal. However, if this same movement data can be linked to e.g. specific workers transporting the product from the warehouse to a retail store, the information classifies as personal data, as it can be used to reveal information on natural persons.

Furthermore, the same ID may be used to monitor the movement of the product, and the consumer carrying it, in a retail store; consequently information on the shopping behaviour can be collected, while a consumer is moving through the store. In case the RFID tag remains active after a purchase, the ID even can be used to re-identify consumers when they re-visit the store and link previously collected data to that person. This means that names of consumers are no longer essential in order to obtain data on their interests and behaviour patterns. If a consumer's identity is revealed at a later point and the purchased product is present, all previously collected data can be linked to the then identified person.

In view of this potential, no clear distinction between personal and non-personal data with RFID systems can be made, since it is not only the main purpose of the application (supply chain management in this example) that is relevant for this classification. In most cases a tag will be linked to an individual.

3.2 Distinction between open, closed and no circulation systems

As illustrated above, a tagged object with a unique ID can not only be linked to personal or non-personal data, it also can easily be referenced in various kinds of applications.

The ID of the product in an “*item level tagging in consumer product supply chain*”-application functions in a “no circulation” system while in the warehouse. In inventory management in a retail store, it is used in a “closed circulation” system; ultimately it enters a “open circulation” system when the consumer leaves the retail store with the product and its enabled RFID tag. The ID can then be accessed by an unknown and uncontrollable number of other RFID applications.

The distinction between open, closed and no circulation-systems requires strict control of where the RFID tag - or the ID stored on the tag - is used. Therefore a complex access control system is needed which allows the usage of a tag only for certain purposes and at the same time denies access to systems with different purposes. Given the limited computing power of RFID tags, such systems are unlikely to be developed in the near future.⁷

Therefore a general “one-size-fits-all” classification of RFID applications, that is based on the extent of the circulation of information, is considered problematic, especially when this classification serves as a basis for risk analysis.

3.3 Classification based on data-protection and user control

EDRi would like to emphasise that the tagging of objects with unique IDs stored on RFID tags always involves the risk of unauthorised collections of personal data unless effective means are installed to restrict access to the information stored on the tag.

⁶ Directive 95/46/EC

⁷ For recent research attempting to hinder hidden readouts of RFID tags see for example: Marc Langheinrich and Remo Marti, Practical Minimalist Cryptography for RFID Privacy, 2007, <http://www.vs.inf.ethz.ch/publ/papers/shamirtags07.pdf> (last visited: 28.05.2007)

EDRi therefore proposes a classification of RFID applications based on data-protection and user control.

While data-protection defines the extent to which the information stored on the tag and in the system can be accessed by different applications, user control defines the extent to which the collection of personal data and the personal data stored in the system can be controlled by the affected natural persons.

It is important to point out that an assessment of barriers and threats especially with regard to Privacy and Security is necessary on a case-by-case basis, as classifications can only provide a general overview over a group of applications with shared characteristics.

	<i>data-protected</i>	<i>data-shared</i>	<i>data-unprotected</i>
<i>user controlled</i>	<ul style="list-style-type: none"> ●information on the tag is stored in a way only interpretable by this specific system ●user controls access to information on the tag ●user controls information related to her/him stored in the system 	<ul style="list-style-type: none"> ●information on the tag is stored in a way only interpretable by a defined set of systems ●user controls access to information on the tag ●user controls information related to her/him stored in the system 	<ul style="list-style-type: none"> ●information on the tag is stored in a way that does not effectively prevent the interpretation by other systems ●user controls access to information on the tag ●user controls information related to her/him stored in the system
<i>user accessible</i>	<ul style="list-style-type: none"> ●information on the tag is stored in a way only interpretable by this specific system ●user has access to information stored on the tag and in the system 	<ul style="list-style-type: none"> ●information on the tag is stored in a way only interpretable by a defined set of systems ●user has access to information stored on the tag and in the system 	<ul style="list-style-type: none"> ●information on the tag is stored in a way that does not effectively prevent the interpretation by other systems ●user has access to information stored on the tag and in the system
<i>user informed</i>	<ul style="list-style-type: none"> ●information on the tag is stored in a way only interpretable by this specific system ●user is informed of the data collection and its purposes but has no direct access to the information 	<ul style="list-style-type: none"> ●information on the tag is stored in a way only interpretable by a defined set of systems ●user is informed of the data collection and its purposes but has no direct access to the information 	<ul style="list-style-type: none"> ●information on the tag is stored in a way that does not effectively prevent the interpretation by other systems ●user is informed of the data collection and its purposes but has no direct access to the information

Table 1: Classification of RFID systems by data-protection and user control

	<i>data-protected</i>	<i>data-shared</i>	<i>data-unprotected</i>
<i>user controlled</i>	Barriers: Privacy/Security: Low Interoperability: Low	Barriers: Privacy/Security: Medium Interoperability: Medium	Barriers: Privacy/Security: Medium Interoperability: High
<i>user accessible</i>	Barriers: Privacy/Security: Medium Interoperability: Low	Barriers: Privacy/Security: Medium Interoperability: Medium	Barriers: Privacy/Security: High Interoperability: High
<i>user informed</i>	Barriers: Privacy/Security: High Interoperability: Low	Barriers: Privacy/Security: High Interoperability: Medium	Barriers: Privacy/Security: High Interoperability: High

Table 2: Barriers to the deployment of RFID applications

3.3.1 User control

The user control criterion defines to which extent the affected person is able to access, correct or delete information stored about her or him.

With **user-informed** applications the user is informed about the collection of data and its purposes only (which constitutes a minimum requirement for any processing of data); to get any further information on the exact kind of data stored on her or him however, the user needs to contact the operator of the application. Furthermore the user has no possibility of control over access to the stored information on the RFID tag or in the system.

With **user accessible** applications the operator of the application provides means for the user to access the data on the tag and in the system; so the user knows which data on her/him is processed by the RFID application at all times. There is still no possibility of control over the access to information stored on the RFID tag or in the system.

User controlled RFID applications finally enable the user to control access to information stored on her/him on the RFID tag. Furthermore the user is also able to control the information related to her/him that is stored in the system. This enables the user not only to access but also to correct and – if necessary – to delete information stored on her or him.

3.3.2 Data-protection

The data-protection criterion defines the extent to which other applications are able to use the information stored on a tag.

With **data-protected** applications the data stored on the RFID tag is only interpretable by the application that the RFID tag was made for. Therefore the information stored on the tag is protected against unauthorised access by other RFID applications and the user's personal data is not distributed to third parties.

Data-shared applications store information on the tag in a way that is interpretable by a defined set of other systems. With data-shared applications the user can get information on which other applications will be able to access the information stored on the RFID tag; the protection of the information against unauthorised access by other applications is guaranteed.

Data-unprotected applications provide no safeguards for the information stored on the RFID tag. Therefore any application is potentially able to access and process this information. With this applications the user is not protected against the distribution of his personal data to third parties.

3.3.3 Barriers

Considering the barriers to the deployment of RFID systems, **user-controlled data-protected systems**

provide the **lowest** potential threats to Privacy, Security and the Interoperability level, because the user is given appropriate means to control access to data stored on her/him and to alter or delete data. Since it is a stand-alone system without aims to share data with other systems, the required interoperability-level is low as well.

Data-shared systems share a **medium level of required interoperability** while threats to **Privacy and Security** are at a **medium to high** level. This is due to the fact that other compatible applications – while limited in number – do not necessarily share the same level of user control and probably are unknown to the user.

The **highest need for interoperability** as well as a **medium to high threat to Privacy and Security** is given in data-unprotected RFID systems. The high-rated threat to Privacy and Security stems from the interoperability level of the applications. As long as the user-control level of the current application does not reach the user-controlled level, the missing protection of the information stored on the tag allows for a widespread usage by any application without the users consent. Only with user-controlled applications the user controls who accesses the information stored on the tag. This contributes to the medium-rated Privacy and Security threat of these applications, despite being data-unprotected.